

ORDER FOR SUPPLIES AND SERVICES				IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution		PAGE 1 OF 1 PAGE(S)	
1. DATE OF ORDER 02/11/2011		2. ORDER NUMBER GST0311DS8011		3. CONTRACT NUMBER GS00Q09BGD0048		4. ACT NUMBER A2469800Z	
FOR GOVERNMENT USE ONLY	5. ACCOUNTING CLASSIFICATION				6. FINANCE DIVISION		
	FUND 299X	ORG CODE A03VR120	B/A CODE F6	O/C CODE 25	AC	SS	VENDOR NAME
	FUNC CODE C01	C/E CODE H08	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
	W/ITEM	CC-B	PRT./CRFT	AI	LC	DISCOUNT	
7. TO: CONTRACTOR (Name, address and zip code) Gregory Parrington SAIC. 10260 CAMPUS POINT DRIVE SAN DIEGO, CA 92121-1522 United States (858) 826-7495				8. TYPE OF ORDER B. DELIVERY		REFERENCE YOUR	
				Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated.			
				This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.			
				C. MODIFICATION NO. 00 TYPE OF MODIFICATION:		AUTHORITY FOR ISSUING	
9A. EMPLOYER'S IDENTIFICATION NUMBER 953630868		9B. CHECK, IF APPROP WITHHOLD 20%		Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.			
10A. CLASSIFICATION B. Other than Small Business				10B. TYPE OF BUSINESS ORGANIZATION C. Corporation			
11. ISSUING OFFICE (Address, zip code, and telephone no.) GSA Region 3 Debra L. Stuart 20 NORTH EIGHTH STREET PHILADELPHIA, PA 19107-3191 United States (215) 446-5817		12. REMITTANCE ADDRESS (MANDATORY) SAIC. PO BOX 223058 PITTSBURGH, PA 15251-2058 United States		13. SHIP TO(Consignee address, zip code and telephone no.) Robert Ayers 5111 Leesburg Pike, Suite 810 Falls Church, VA 22041 United States (703) 681-7125			
14. PLACE OF INSPECTION AND ACCEPTANCE Naomi Escoffery 5113 Leesburg Pike Suite 701 Falls Church, VA 22041 United States		15. REQUISITION OFFICE (Name, symbol and telephone no.) Ibrahiim Kent GSA Region 3 100 PENN SQUARE EAST PHILADELPHIA, PA 19107-3322 United States (215) 446-5825					
16. F.O.B. POINT Destination		17. GOVERNMENT B/L NO.		18. DELIVERY F.O.B. POINT ON OR BEFORE 02/13/2015		19. PAYMENT/DISCOUNT TERMS NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS	
20. SCHEDULE							
<p>Cost plus Fixed Fee task order number GST0311DS8011 is issued for AHLTA and CHCS Critical Fixes and Support in accordance with the Government's Statement of Objectives (SOO) and the contractor's cost proposal (b) (4) dated February 25, 2010 in the amount of (b) (4) inclusive of all potential optional CLINS and all potential option years and the contractor's technical proposal dated February 25, 2010 coupled with the contractor's oral presentation of March 16, 2010. The base period of performance for this task is February 14, 2011 to February 13, 2012 for Base Tasks 1-5. The total estimated value of the base year is (b) (4); this amount includes the (b) (4) Alliant Contract Access Fee for the base year.</p> <p>This task order also includes 3 one-year optional periods of performance through February 13, 2015 to be exercised at the unilateral right of the Government.</p> <p>This task order is incrementally funded in the amount of (b) (4). It is anticipated this funding will support effort through 8/31/2011.</p> <p>Base year fixed fee is (b) (4). Total fixed fee inclusive of all optional items and all optional periods is (b) (4).</p> <p>Total Alliant Contract Access Fee inclusive of all optional items and all optional periods is (b) (4).</p> <p>The contractor shall submit a revised cost proposal by February 28, 2011 reflecting current indirect rates including subcontractors where applicable. Rates shall be supported by the cognizant audit agency, i.e., DCAA or DCMA. Subcontractor information may be submitted directly to the Contracting Officer.</p>							
ITEM NO. (A)	SUPPLIES OR SERVICES (B)			QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
(b) (4)							

STATEMENT OF OBJECTIVES (SOO)
for
United States Department of Defense (DoD)
TRICARE Management Activity (TMA)
AHLTA & CHCS Critical Fixes and Support

Task type: Alliant, Cost Plus Fixed Fee

1.0 SCOPE

This Statement of Objectives (SOO) outlines the goal of the Department of Defense (DoD) to improve the current electronic health record (EHR) by addressing existing technical and functional EHR challenges. It identifies the necessary fixes to the legacy EHR systems and architecture so that the EHR capability will be more reliable, stable, user friendly and perform with adequate speed. The SOO also describes the new capabilities that need to be implemented in support of the CAPT James A. Lovell Federal Health Care Center (formerly JALFHCC currently FHCC NC) in North Chicago, IL, which includes Single Sign-on (SSO) Government Furnished Information (GFI), Patient Registration, Orders Portability (Pharmacy, Laboratory, Radiology, and Consults/Referrals) and Operational Readiness. The intent of this SOO is for comprehensive development, integration, testing, deployment, and initial sustainment.

1.1 Background

The current DoD EHR was built and relies upon late 1980s and 1990s technologies. To meet evolving user's needs, EHR enhancements are routinely released. The DoD EHR has continued to evolve and mature since its inception in the 1990's to where it is now. The DOD EHR is the largest ambulatory EHR in the world, with the documentation of an average of 140,000 patient encounters each day. However, the current suite of EHR applications and underlying infrastructure do not support the challenges of the rapid evolution of today's healthcare practices, the ever-increasing need to transact and share data across the continuum of care, and the timely fielding of new capabilities. There are significant technical and functional EHR problems that adversely affect the reliability, speed, usability, and data integrity of the overall system which has resulted in dissatisfaction with the EHR throughout the DoD healthcare community at large. Existing applications were built at different times, use different standards and terminologies, and even though interfaced, look different to the user and perform differently. Because there is no common dictionary of terms in use by these legacy systems, continuous mapping of terms is required, significantly impacting maintenance costs. From the user's perspective, the EHR doesn't function as one product but rather several products, requiring multiple log-ins, memorization of different screens and placement of key functions, and time consuming movement between the various applications. The number of interfaced applications drives up the cost and time to develop and test new capabilities. Instead of developing a product to interface with one system, it requires developing a product to interface with many applications. Additionally, changes to the aging hardware, software, workstations, servers, and communications networks often impact the system's performance, making it more unreliable and slow. Consequently, the EHR and its interfaced legacy systems face issues of sustainment, reliability, extensibility, scalability, interoperability, usability, extended development timelines, and capability gaps.

The following summarizes the challenges of the current system.

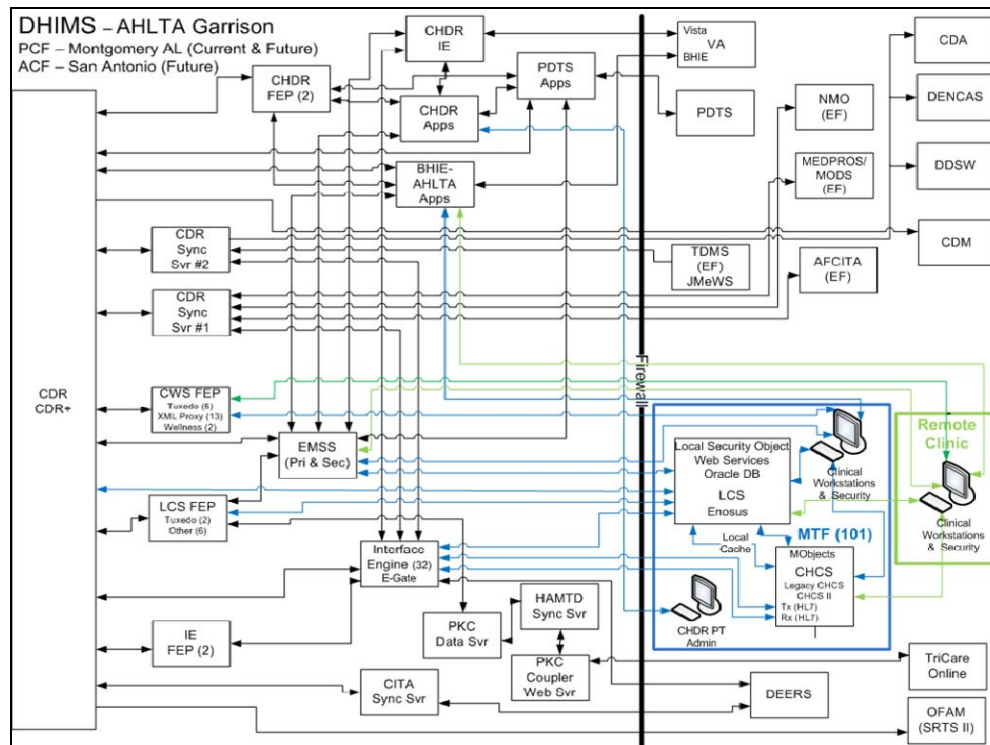
- Fragmented architecture
- Disparate data dictionaries
- Many points of failure
- Complex inter-connections
- Disparate systems & interfaces
- Resource intensive design
- Slow system performance
- Antiquated technology (20+ Years old)

In short, the antiquated technologies and legacy system underpinnings of the current EHR hamper the Military Health System's (MHS) ability to meet DoD's wartime demands and our users' expectations of rapidly fielded, reliable and usable information technologies that support the delivery of healthcare services whenever and wherever needed. Additionally, antiquated technology hinder our ability to meet increasing demands from the DoD wartime challenges, including improved healthcare information management for our Wounded Warriors, to our stakeholders' expectations of rapid, timely delivery of information technologies that support the provision of healthcare services.

Current System Overview

The current architecture is complicated with multiple points of failure. APPENDIX H – Problem Description for the EHR Architecture describes some of these points of failure. APPENDIX J – Architecture Diagrams documenting the current system [provides more detailed diagrams](#).

Deleted:



There are obsolete technologies and an aging infrastructure that operates in an environment that competes for resources, licenses and functionality. The grid groups some of the challenges that are identified in the architecture above.

Issue	Speed	Reliability	User Interface	Data Integrity	Scalability	Time to Market	Interoperability	Sustainability	Resource Intensive
Most AHLTA changes require installation on all clinical workstations		x			x	x		x	x
User Interface is not Intuitive			x						
AHLTA Requires Extensive System Resources on the clinical workstation	x				x	x		x	x
Multiple Logons Required to Access EHR Applications	x		x		x				
Security Solution is Inadequate and Problematic	x	x			x			x	
Shared Administrative Account				x				x	
Unsupported Oracle code	x					x		x	
Architecture is not IPv6 Compliant							x		
LCS is not fault tolerant		x							
Tightly Coupled Access Between CHCS & LCS	x	x					x	x	
Cost to perform and continue data mapping is high			x		x			x	x
Outdated CHCS Architecture and User Interface			x				x	x	
Duplicate Patient Record		x		x				x	x
Current antiquated 3M Architecture limits EHR capability		x						x	
No Automated CDR Failover		x						x	
CDR is a Single Point of Failure		x						x	
CDR Database Manageability	x	x			x			x	x
Unsustainable CDR-CDM Interface		x			x	x	x	x	x
CDR Synch Servers not scalable	x	x			x			x	
Interface Engine Architecture is not Highly Available or Efficient		x			x			x	
Unable to associate images and artifacts with a patient's EHR			x		x			x	
Degraded BHIE-AHLTA Performance	x							x	
BHIE-AHLTA Does not have a Standard Interface for Exchanging Data	x		x			x	x		x
Expeditionary Framework uses Non Standard Ports and is Unidirectional		x						x	
AHLTA Dedicated Network (COI) expensive and non-redundant		x						x	
No Production-Like Test Environment	x	x				x		x	

There is a number of architecture challenges of which a sample of the issues currently faced with today's architecture are listed below.

- Most AHLTA changes require installation on all clinical workstations – Changes/upgrades must be performed on each of the 110,000 workstations.
- The User Interface requires too much mouse clicking to navigate through AHLTA.
- AHLTA loads workstations with too many processes and use too many system resources.
- Users must login more than once to more than one application to accomplish certain task.
- More than one security/access solution is used for multiple applications. Snareworks is a frequent cause of denied access to AHLTA due to software failures.
- Some AHLTA applications are running on the LCS as foreground applications dependent upon the administrator to be logged in to function. LCS cannot be logged out of without loss of functionality resulting in reduction in accountability due to common administrative account and password being shared with multiple administrators and applications.
- AHLTA Client has unsupported Oracle code.
- Data transmission on networks must use the IPv6 format.
- The ability of the LCS to continue operating in the event of failure has not been addressed.
- If CHCS or LCS is not functioning, AHLTA will not allow users to operate.

- Poor understanding of the data mapping processes is leading to higher sustainment costs and inability to leverage additional benefits.
- CHCS as an older “legacy” platform which causes difficulty when trying to update anything it is connected to.
- Too many duplicate patient records which are expensive to resolve.
- Non-current 3M versions make sustainment more difficult, decreases availability and increases time-to-market.
- Lack of automated offline failover capability causes significant delay recovering from an outage.
- Current CDR Architecture provides for lower availability and potential for data loss.
- Exponential growth rate of CDR storage causes manageability issues.
- Lack of Database management/maintenance causes performance issues and fragmentation.
- CDR-CDM interface is based on legacy proprietary code that is hard to manage and maintain.
- Performance impact to CDR transaction system.
- Current CDR-CDM interface causes system resource overhead to the CDR transactional system.
- Errors created by changes to the CDR not capture in the CDM.
- Architecture is not scalable.
- CDR Synch Server#2 (CSS2) is not able to ingest the backlog of Theater records or support the current incoming load.
- In the next quarter, multiple additional sources from Theater will be sending data through CSS2 to the CDR.
- The CHCS host being mapped to a single corresponding e*Gate makes failover to the Alternate Computing Facility (ACF) a manual process.
- Each e*Gate server services only three to four individual CHCS hosts providing a single point of failure and no load balancing capability.
- No mechanism for adding, viewing, storing, or maintaining artifacts and images (e.g., radiology, pathology, dermatology, ophthalmology) associated with a patient’s EHR.
- Lack of a standard means of communication causes difficulty interfacing with other systems.
- Lack of a standard means of communication causes difficulty interfacing with other systems.
- Theater messaging does not scale well toward the top of the tree, where message traffic is very high. This leads to no guarantee messaging and to no intelligent transfer.
- Fragmented data.
- Difficult and often complicated data sharing.
- Data architecture that does not adequately support the capability need.

AHLTA Size and Usage Levels

- CDR Database Load Profile

	Per Second

Redo size:	15,018,838.80
Logical reads:	1,836,210.20
Block changes:	86,633.98
Physical reads:	28,050.50
Physical writes:	2,220.93
User calls:	46,385.73

Parses:	13,194.96
Hard parses:	99.29
Sorts:	17,878.23
Logons:	2.45
Executes:	31,511.76
Transactions:	1,206.94

- Daily encounters 150,000
- Daily HL7 messages 2,000,000
- Peak user count 16,500
- Database Size _____64 Tb
- Database growth rate per month____1.5 Tb
- 77,000+ active users
- 110,000+ end user devices
- 9.5 million beneficiaries with clinical data
- Covers every time zone
- **Military Treatment Facilities**
 - 63 Hospitals
 - 413 Medical Clinics
 - 375 Dental Clinics

Theater size and usage levels:

- TMIP-Block 2 to all their locations 1 Aug 2009 completed all theater hospitals with Block 2
 - 15 Theater Hospitals,
 - 262 Forward Resuscitative sites
 - Aboard 9 U.S. Naval Ships
 - 7.93 million orders of ancillary services (laboratory, radiology, pharmacy)
 - 2.78 million outpatient encounters captured in AHLTA-Theater

Inpatient size and usage levels:

- 24 Sites
- 56% Inpatient Beds

Coordination with VA and other entities

The Contractor will work closely with the Integrator to complete the tasks outlined in this SOO and is expected to propose a co-operative strategy to eliminate duplication of efforts, maximize existing resources, and at the same time, mitigate risks associated with dependencies from supporting integration activities that may be provided by a separate Contractor. Coordination shall include the following entities:

- AHLTA/CHCS Integrator (SAIC)
- AHLTA-Theater Integrator (SAIC)
- National Health Information Network

1.2 Transition Support

The Contractor will provide 90 days of outgoing transition for transitioning work from an active task order to a follow-on contract/order or Government entity. This transition may be to a Government entity, another Contractor or to the incumbent contractor under a new contract/order. In accordance with the Government-approved plan, the Contractor will assist the Government in planning and implementing a complete transition from this Contract and/or orders issued under this Contract to a successful provider. This may include formal coordination with Government

staff and successor staff and management. It may also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This transition may include, but is not limited to:

- Coordination with Government representatives,
- Review, evaluation and transition of current support services,
- Transition of historic data to new contractor system,
- Government-approved training and certification process,
- Transfer of hardware warranties and software licenses,
- Transfer of all System/Tool documentation to include, at a minimum: user manuals, system administration manuals, training materials, disaster recovery manual, requirements traceability matrix, configuration control documents and all other documents required to operate, maintain and administer systems and tools,
- If another contractor follows this contractor with work related to this work, this contractor will provide any developed source code (compiled and uncompiled, including all versions, maintenance updates and patches) with written instructions for the source code on which this contractor has worked, so that an experienced software engineer, previously not familiar with the source code can understand and efficiently work with the source code. In addition, this contractor will provide for 90 days, a software engineer (or person of comparable work level) with significant experience working with the source code, to assist the new contractor,
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
- Disposition of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.,
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance,
- Applicable TMA debriefing and personnel out-processing procedures,
- Turn-in of all government keys, ID/access cards, and security codes.

1.3 Organizational Conflict of Interest Category

TRICARE Management Activity (TMA) has categorized all its non-purchased care requirements into three broad categories, as defined below, for purposes of identifying, avoiding or mitigation against Organizational Conflicts of Interest (OCIs) in accordance with Federal Acquisition Regulation (FAR) Subpart 9.5. These categories are defined as follows:

- Category 1: TMA Internal Support: Services which, by their very nature, give the Contractor access to extensive data about the contracts of all other TMA Contractors.
- Category 2: Program Management Support: Services which assist TMA in planning and managing its activities and programs. This includes, for example: requirements analysis, acquisition support, budget planning and management, business process reengineering, program planning and execution support, and independent technical management support.
- Category 3: Product Support. Services or end items required to meet the mission requirements of TMA's non-purchased care activities and programs. This includes, for example: concept exploration and development; system design; system development and integration; Commercial-off-the-shelf (COTS) procurement and integration; internal development testing; deployment; installation; operations; and maintenance.

Contractor participation in more than one of these areas may give rise to an unfair competitive advantage resulting from access to advance acquisition planning, source selection sensitive or

proprietary information. Furthermore, Contractor participation in more than one area may give rise to a real or apparent loss of Contractor impartiality and objectivity where its advisory or planning assistance in one area potentially affects its present or future participation in another area.

The purpose of this categorization is to accomplish the following three objectives: (1) to inform prospective Offerors that TMA presumes that award of a contract or order in the subject category will give rise to real or apparent OCIs with respect to requirements in the other two categories; (2) to assist current Contractors and prospective Offerors in developing their own business strategies regarding participation in TMA requirements and in identifying and, where possible, avoiding or mitigating against OCIs; and (3) to ensure that all current Contractors and prospective Offerors are afforded the maximum practicable opportunity to compete for all TMA requirements consistent with the restrictions required under FAR Subpart 9.5 and sound business practices.

For purposes of identifying, avoiding and / or mitigating against OCIs, TMA will examine all its non-purchased care requirements and acquisitions regardless of the cognizant contracting activity (e.g., Defense Contracting Command-Washington (DCC-W), General Services Administration (GSA), other agency Multiple Award Schedules) or the type of contract vehicle used (e.g., FSS order, Fair Opportunity competitive order under Multiple Award ID/IQ Contracts, competitively negotiated awards under FAR Part 15).

Each TMA non-purchased care solicitation will therefore be designated as falling within one of the three above defined categories. The work called for under this contract / order has been categorized by TMA as a non-purchased care task as **Category 3: Product Support**.

An Offeror that has never provided support to TMA in any of the categories is eligible for award in any category without any further action required under this clause.

An Offeror that provides or has provided support to TMA in only one category of work and has never supported TMA in any other category (a single-category Contractor) is eligible for award for any future requirement in that single category without further action under this clause.

A single-category Offeror/Contractor that submits an offer in a different category, or any Offeror/Contractor which now provides or previously has provided support in more than one category, is eligible for award if the Offeror submits a comparative analysis and, if necessary, an OCI Avoidance or Mitigation Plan, and the Contracting Officer determines that no OCI would arise or that the OCI Avoidance or Mitigation Plan adequately protects the interests of the government in the event of award to that Offeror.

2.0 STATEMENT OF OBJECTIVES

System Objectives

- Stabilize the present system sufficiently to ensure future transition to new capabilities or re-use in a larger enterprise EHR architecture modernization effort.
- Stabilize AHLTA/Composite Health Care System (CHCS) for high reliability and availability.
- Significantly reduce the need for data mapping maintenance.
- Improve system performance from the perspectives of the clinical end user and system administrator.
- Integrate AHLTA and CHCS into a single cohesive, modular and portable health system using industry best practices and a service oriented approach. Leverage Single Sign On and Context Management (SSO/CM) for functions that are not integrated into this single cohesive system. Ensure that new capabilities are integrated with and added to the recently selected Citrix PasswordManager for SSO and CareFx for CM.
- Eliminate the top defects and security vulnerabilities at their root cause in APPENDIX A- EHR System Defects and Service Change Requests (SCRs).
- Reduce the complexity of the existing computing framework while increasing the availability, maintainability, and performance. Maintain local off-line functionality (e.g., document care) and eliminate single points of failure e.g. inline caches among a number of other points described.
- Extend the Garrison capabilities in a common baseline to the Theater of Operations to provide a “train as you fight” user experience in the system. The Theater based system should have the same look, feel and baseline functionality however operate in an austere environment with limited computing, communication and system administration resources.
- Eliminate duplicative (e.g., Multiple database technology) and divergent technology (e.g., specialty, non-mainstream Operating Systems).
- Fully expose the EHR data to the Business Objects suite to allow for enhanced reporting capabilities.
- Implement standards-based approach for health information exchange between current EHR capabilities in the MHS using Service Oriented Architecture (SOA) principles.
- Provide a comprehensive and integrated view of health history and access to all EHR capabilities using a modular, configurable framework.
 - Enable data sharing by exposing all data as web services, both for existing sharing mechanisms such as Bidirectional Health Information Exchange (BHIE) and new sharing initiatives.
 - Share information in support of national initiatives such as Nationwide Health Information Network (NHIN) using standards such as the Healthcare Information Technology Standards Panel (HITSP).
 - Integrate the users health information management picture into a common graphical user interface (GUI) using a modular and portable approach that includes the images and artifacts in current EHR applications such as Essentris®, Neurocognitive Assessment Tool (NCAT), Behavioral Health (BH) and Healthcare Artifact and Image Management System (HAIMS).
 - Ensure all inpatient and outpatient Theater data is available in the clinical workflow. Theater patient data should be available when the patient presents to the Sustaining Base Military Treatment Facilities (MTF) for care.
- Reduce the level of effort required to deploy and maintain the system and its components by simplifying the architecture.

- Support multi-year code sets (e.g., International Classification of Diseases (ICD), Current Procedural Terminology (CPT), Current Dental Terminology (CDT)).
- Adhere to industry guidelines for distributed and load balanced architecture to increase redundancy, availability and workload balancing.
- Reduce the use of custom software and implement off the shelf technology that requires little or no code modifications (e.g., user authentication and authorization).
- Align the system with MHS Internet Protocol version 6 (IPv6) and MHS Public Key Infrastructure (PKI) requirements.
- Leverage new functionality from the pre-production AHLTA 4.0 baseline and incorporate into Sustaining Base and Theater baselines (APPENDIX C-AHLTA 4.0 Prototype Baseline Functionality). AHLTA 4.0 pre-production source code, binaries, and documentation will be provided as GFI.
- Minimize the client install footprint.
- Leverage automated duplicate patient reduction solution.
- Leverage Defense Manpower Data Center (DMDC) patient identity management services.
- Leverage Tri-Service Infrastructure Management Program Office (TIMPO) joint active directory service for user identity management.
- Leverage existing software, where applicable, that is reliable and employs sound engineering design and maintenance standards.
- Ensure all essential capabilities also operate in austere environments such as the Theater of Operations.
- Expose health information data as standards based services to improve data sharing for the Department of Veterans Affairs (VA) and NHIN.
- Simplify and unify modes of operation. Example capability matrix with complexity of pre-production AHLTA 4.0 baseline operation that needs to be simplified illustrated in APPENDIX B – AHLTA 4.0 Prototype Capability Matrix.
- Enable the client application to run on DoD approved operating systems platform.
- Enable all server based systems to operate on DoD approved x86 hardware architecture (in a 64 bit environment where applicable).
- Eliminate current stovepipes through the design and implementation of an enterprise approach to health information management so that capabilities are available globally (e.g., orders and results) at any MTF and locally during an offline failover.
- Provide reach-back access to health history when a network connection is available for an integrated enterprise view for both Sustaining Base and Theater (e.g., orders and results).
- Ensure availability of up-to-date computable clinical data for clinical decision support in both the Sustaining Base and Theater (e.g., enterprise drug checks).
- Maximize use of virtualization technologies where applicable (licenses will be Government Furnished Equipment (GFE)).
- Comply with MHS Information Assurance requirements (APPENDIX D- MHS Information Assurance Requirements).
- Maximize interoperability and data sharing while adhering to data and messaging standards (APPENDIX E- Enterprise Architecture Standards).
- Recommend for removal obsolete modules or non-functional code and only remove upon government approval.
- Obtain the information for a common user interface by exposing data through the MHS Enterprise Service Bus (ESB) framework through common industry compliant, reusable web services with the following considerations:

- Web services should behave in a standardized way; integrating applications using Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Service Definition Language (WSDL), Web Services for Remote Portlets (WSRP 2.0), Asynchronous JavaScript and XML (AJAX), requires client-side certificates, utilize secure sockets layer (SSL) for secure and encrypted data transfer and Universal Description Discovery and Integration (UDDI) open standards over an Internet protocol backbone.
- There are currently some DoD web services that expose information from some of the systems; however, they all require modernization to become compliant with industry standards.
- Provide the capability to run on Microsoft XP, Vista and Windows 7
- Operate on current standard MHS Infrastructure with a Network Protection Suite at each host site and appropriately sized bandwidth based upon capacity models for the systems the network supports
- Network characteristics are 99.5% availability, no more than 200 milliseconds latency CONUS, and no more than 350 millisecond latency OCONUS. The MHS Community of Interest network (COI) provided by DISA meets the above performance measures. This does not take into account the DoD installation networks which are controlled by the Services. Theater is not included.

Program Objectives

- Integrate, test, deliver and implement the capabilities identified within the SOO and specifically detailed in the Systems and Design/Engineering Objectives in a 12 month period with no more than 6 months between deliveries.
- Consider the current DoD and VA architecture and infrastructure at FHCC NC).
- Coordinate with the VA for technical solution for FHCC NC.
- Meet the FHCC NC Functional Requirements that are contained in the MHS Dynamic Object Oriented Requirements Systems (DOORS) Repository, Baseline 01 June 2009, and included in Appendices to this document with a solution that will enable data interoperability between DoD and VA systems and that can be scaled to meet enterprise demands. The licenses for deployment of the portal and ESB frameworks will be GFE.
- Design, develop, document, test, and demonstrate a revised AHLTA/CHCS system that meets the requirements specified in the Systems Requirements Document (SRD).
- Implement Capability Maturity Model Integration (CMMI) V1.2 into the processes used to develop the revised AHLTA/CHCS system.
- Develop, document, and implement effective software development plans, processes, and capabilities in accordance with the International Organization for Standardization/International Electro-technical Commission (IOS/IEC) Final Draft International Standard (FDIS) 12207 Institute of Electrical and Electronic Engineers (IEEE) Std 12207-2007, Systems and Software Engineering Software Lifecycle Processes, necessary to achieve program objectives and provide for thorough lifecycle software support.
- Demonstrate technical and design maturity at program decision points including the System Requirements Review (SRR), Preliminary Design Review (PDR), and Critical Design Review (CDR) milestones.
- Employ comprehensive program management to identify, analyze, plan, track, control, communicate, and document significant technology, performance, cost, schedule, integration, producibility, risks, and other issues. Participate in and leverage industry and Government-sponsored risk mitigation activities as appropriate.

- Plan and implement a robust and disciplined hardware and software test and evaluation program using the government's common development and testing environment to validate the designed system and sub-systems meet the SRD.
- Ensure development and evolution of a supportable system design that assures future implementation of an affordable and comprehensive integrated logistics support capability necessary to support program objectives and sustain operational and support cost requirements.
- Update training manuals and computer based training to reflect the fixed functionality/enhancements.
- Ensure maximum synergy, reusability and efficiency in support of vendors addressing AHLTA stabilization, BHIE 5 and sustainment project services.
- The Government will conduct static and dynamic code quality checks using Contractor provided source code and compiled code.

Design/Engineering Objectives

The Contractor is encouraged to present a number of options that may include software repairs, software re-write, code conversion (including automated), web service wrapping, new COTS integration or any combination that will result in a simplified but far more reliable, faster and scalable architecture that help transition the MHS into the future state in a follow on phase. Significant consideration will include industry best practices, stability, scalability, reusability, architectural simplicity, reduced footprint, enterprise data and document availability, reduction in duplicate functions, interoperability with health standards, and reduction in maintenance/sustainment. The Government prefers incremental deliveries with the final delivery objective in 12 months but no later than 18 months from date of award.

It is the Government's goal to deliver the full solution in support of the FHCC NC (requirements attached at Appendix F), by the opening day of October 1 2010. The Government will consider innovative solutions for FHCC NC that will be an initial building block(s) with the final solution delivered by the end of the contract Base year period of performance. Although providing a solution to support the FHCC NC requirements in the given timeframe is an objective, the government understands that this may not be achievable given the timeframe available for development. It is the priority of the Government to acquire high quality software that is open architecture, non-proprietary in nature leveraging COTS where applicable rather than developing quick, potentially unstable solution(s) that may present problems in the effort to repair AHLTA & CHCS. The Government is looking for principles of modular, scalable open systems architecture as a strategy to facilitate affordable and supportable system development and modernization of fielded assets.

The threat of identity theft has become increasingly common due to the overuse of Social Security Numbers (SSNs). Therefore, all Federal agencies are to evaluate their use of SSNs. For the purposes of the Department of Defense (DoD), the Office of the Under Secretary of Defense released Directive-Type Memorandum (DTM) 07-15-USD (P&R), "DoD Social Security Number (SSN) Reduction Plan", 28 March 2008. The Contractor will comply with this directive in their design to limit the use and visibility of SSN to help prevent identity theft and use the DoD identifier. During this transition, legacy systems such as AHLTA/CHCS will be capable of searching by SSN and the Electronic Data Interface Personnel Identification (EDI PI). In addition, all DoD Beneficiaries will also have a DoD benefits number that is tied to their sponsor and health benefits. The AHLTA/CHCS system should allow for searching and displaying of the EPI PI and DoD Benefits number. More information about this requirement and the plan within

the DoD can be found here: <http://www.cac.mil/> The vendor will consider these actions in accordance with the DoD implementation plan of SSN reduction.

- Remove the SSN from barcodes and display on DoD ID cards. (The removal of dependent SSNs from ID cards is already underway. Removal of SSNs imbedded in barcodes will occur by 2012.)
- Remove or reduce use of SSNs and PII from DON forms, where feasible. Collection must be validated against a list of authorized exceptions.
- Reduce the electronic display, storage and transmission of SSNs and PII.
- Collect and report actions taken to reduce/eliminate use of SSNs to DoD.
- Ensure 100 percent of IT systems that collect SSNs and other PII have completed a Privacy Impact Assessment.

2.1 Objective Set 1 – Federal Health Care Center (FHCC) Enterprise Data Sharing

DoD and VA will be utilizing an integrated information system at the Federal Health Care Center (FHCC NC) in North Chicago, IL. Regardless of whether the patient is a currently in DoD or VA, relevant information has to be shared transparently between both systems. Health care providers will be able to leverage functionality in new and legacy systems from both DoD and VA through a common graphical user interface. The core areas in this objective to be addressed by information systems support for the new FHCC NC include Single Sign-on (GFI), Patient Registration, Orders Portability (Pharmacy, Laboratory, Radiology, and Consults/Referrals) and Operational Readiness as addressed in the FHCC Functional Requirements contained in the MHS DOORS Repository, Baseline 01 June 2009, and included in APPENDIX F-FHCC Functional Requirements.

Deleted: CAPT James A. Lovell

Deleted: in time for the facility's opening on October 1st, 2010

Dependencies: Completion of this objective is dependent on parallel development of FHCC-related components in Objective 2 – Leverage Enterprise Service Bus and Objective 3 – Leverage Enterprise Portal Framework.

Statement of Need:

- Develop, integrate, test, and implement upgrades to the existing MHS applications (i.e. AHLTA, CHCS, CHDR, and Bidirectional Health Information Exchange (BHIE)) to support a DoD/VA integrated information system at FHCC NC.
- Develop, integrate, test and implement a common patient registration capability that allows the authorized user to create, update, and view patient registration in a manner that provides a unique patient identity, validates patient eligibility and enrollment status, and collects necessary information needed for appropriate billing of services:
 - Use a minimum set of demographic data from Defense Enrollment Eligibility Reporting System (DEERS) and VA enrollment systems to complete patient registration and create a unique patient file in both the DoD and VA systems of record.

Deleted: in time for the facility's opening on October 1, 2010

Note: The 4-way reconciliation of patient identity between CHCS, Veterans Health Information Systems and Technology Architecture (VistA), DEERS and the Master Patient Index (MPI) is currently being completed at the enterprise level and is not within the scope for this effort.

- Support a single patient registration process regardless of whether the patient receives care from a DoD or VA provider.
- Present a common registration solution through a single, shared Patient Registration GUI or portlet interoperable with the VA and leveraging current functionality.
- Leverage an enterprise Common Patient Lookup Service to query registration systems and enterprise identity sources that allows users to enter search criteria to

retrieve demographics from the DoD and VA enrollment/registration systems; allow the user to select a single patient from the results and register the patient in both CHCS and VistA with a single action.

- The solution should synchronize updates between CHCS and VistA and leverage existing batch registration functionality in CHCS to trigger registration in VistA.
- Leverage specific enterprise identity sources for FHCC NC: DEERS for DoD beneficiaries and MPI for VA Beneficiaries.
- Ensure that one and only one equivalent record exists in both DoD and VA.
- Manage and/or utilize mapping between unique patient identifiers from each MPI for each registered patient to support Patient Context Management as well as Ancillary Order Portability.
- Extend current legacy application capabilities to allow DoD and VA healthcare professionals to manage laboratory, radiology, pharmacy, and consult orders portability between AHLTA and VistA.
- The solutions must support both the immediate needs at the FHCC NC, and become reusable in future VA/DoD collaborative ventures by ensuring compatibility with other MHS objectives described in this SOO.
- The solution should utilize a Terminology service to translate data elements between DoD and VA format if necessary.
- Processing exceptions should generate alerts to the user with meaningful information to resolve the exception.

2.2 Objective Set 2 – Leverage Enterprise Service Bus

This objective leverages the government furnished MHS EHR ESB framework to enhance data sharing and interoperability between the MHS, VA, FHCC NC and NHIN. The government will provide an open standards ESB when available. To support this, common tables, services, terminology and schema documents must be developed and be accessible from the ESB. The UDDI must be populated with all developed common services. Additionally, the capability to transform HL7 messages from the current legacy versions to other versions of HL7 such as Clinical Documentation Architecture Release 2 (CDA R2) must be implemented. The vendor must configure the necessary services to support the relevant activities within this SOO to support a service oriented approach.

Dependencies: Completion of FHCC-related components in this objective are required for successful completion of Objective 1 – Federal Health Care Center. This objective is anticipated to be completed in parallel with Objective 3 – Leverage Enterprise Portal Framework.

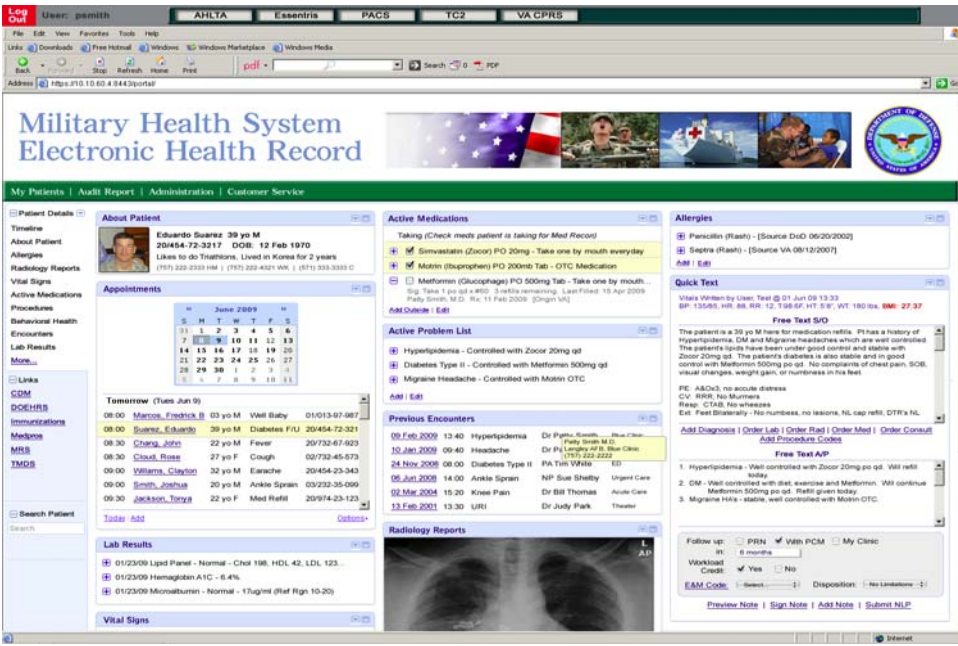
Statement of Need:

- Configure and implement appropriate and necessary services in support of relevant activities in this SOO by leveraging the MHS ESB infrastructure, as deployed by TIMPO and provided as GFI when available, to enhance all aspects of MHS system integration, system decoupling, sustainability, manageability, and help achieve the MHS's goal of a service oriented architecture to:
 - Support activities where applicable within this SOO.
 - Support the data sharing and interoperability between the MHS, VA and NHIN.
 - Publish common schema documents, such as the HITSP XML schema files (i.e. C32) to provide the enterprise with a library industry schema documents.
 - Implement the “MHS Common Tables and Terminology” that can be leveraged by all MHS applications using Unified Medical Language System (UMLS) where applicable. These tables, include but are not limited to the following:

- ICD-9
- CPT
- Logical Observation Identifiers Names and Codes (LOINC)
- Systematized Nomenclature of Medicine (SNOMED)
- Common International Organization for Standardization (ISO) standards tables (e.g., State abbrev., Country codes, ZIP)
- Common HL7 Defined data-sets (e.g., gender codes)
- Handle semantic and syntactic information interoperability.
- Manage messaging that ensures ESB access via use of XML-based protocols such as Web Services Notification (WSN), UDDI, Representational State Transfer (REST), and SOAP.
- Handle message and transaction validation in order to ensure operational integrity.
- Provide for routing of HL7 messages originating from EHR to multiple destinations.
- Provide capability to transform HL7 messages.
- Vendor shall publish their developed services in the UDDI repository.
- Provide semantic interoperability services to support a common syntax and terminology within the MHS enterprise and between the MHS and external trading partners.
- Ensure the security, integrity, availability, and confidentiality of all data and applications that employ the ESB and future SOA common services.
- Facilitate and support implementation of MHS SOA business process services to service subscribers, and to provide components of an MHS Service Oriented Infrastructure (SOI).
- Implement an enterprise identity management service on the ESB as an enterprise common service.
- Implement a patient look-up service, or services, as an enterprise common service.

Objective Set 3 – Leverage Enterprise Portal Framework

This objective provides a common web user interface using the government furnished portal framework which will host discreet pieces of functionality through standards compliant portlets which the vendor must develop to the standards and configure to support the appropriate objectives in this SOO. These portlets must be created by the vendor to implement into the portal framework (GFI) in order to present a consistent and comprehensive view of patient data across the enterprise including relevant data from the VA and external sources as notionally represented below:



Dependencies: Completion of FHCC-related components in this objective are required for successful completion of Objective 1 – Federal Health Care Center. This objective is anticipated to be completed in parallel with Objective 2 – Leverage Enterprise Service Bus.

Statement of Need:

- Provide access through the GUI to the current EHR capabilities which includes AHLTA, CHCS, clinical case management solution, disability evaluation system solution, HAIMS, NCAT, TBI/BH, Essentris, medication reconciliation and IBM Workplace forms (to include Theater systems).
 - Available portlets and links for MHS (and potentially VA) consumption, expanding upon common services being developed under separate action (BHIE Release 5) must be accommodated. These include but are not limited to the following.
 - The FHCC portlet for single patient registration and orders portability for the purpose of DoD and VA viewing.
 - Complete and comprehensive AHLTA/CHCS health history in portlets such as immunizations & consults and administrative data such as notifications and scheduled appointments.
 - Integrate Essentris health history Web service to present for viewing in the clinical workflow as notional depicted above.
 - Incorporate GFI portlets e.g., NCAT, DES, HAIMS, TBI/BH, PKC Couplers, Enterprise Wide Scheduling and Registration (EWSR), and TC2 GUI.
 - Incorporate links to MHS Systems such as DMHRSi, DoD Global Emerging Infections System, DoD Occupational and Environmental Health Readiness System (DOEHRs), Defense Medical Epidemiology Database, TRICARE Online, Medical Protection System (MEDPROS), Medical Readiness Reporting System (MRRS), AFCITA, Personal Information in Medical Research (PIMR), MEDPROS Periodic Health Assessment (PHA), Corporate Dental Application

(CDA), Dental Common Access (DENCAS) and Dental Data System-Web (DDS-W).

- Incorporate links to references such as Armed Forces Medical Intelligence Center, MHS Learn, Military Vaccines (MILVAX), U.S. Army Medical Department Homepage, Navy Medicine Online Portal, Air Force Medicine, Armed Forces Medical Library, Practice Guidelines Home Page, Stimson Library, Travax EnCompass, AHLTA Community Driven Best Practices, Medical Communications for Combat Casualty Care (MC4) – Training, Deployment Health and Up To Date.
- Incorporate links to Reporting tools such as the Clinical Data Mart (CDM), MHS Population Health Portal, Army Medical Department (AMEDD) Command Management System and Air Force Surgeon General Analyst Support.
- The common EHR workflow must be integrated by enabling all EHR products to work seamlessly with SSO/CM products provided as GFI to gain access within the workflow to other EHR support systems that are not Java Specification Request (JSR) 168/286 or Web Services for Remote Portlets (WSRP) 2.0 compliant to operate in the framework.
- The GUI must provide access and display of comprehensive summaries of patient demographic data from local and enterprise identity management resources.
- The GUI must be capable of integrating with the existing infrastructure and major applications without significant impact or changes.
- The GUI must comply with the portal framework SSO and Clinical Context Object Workgroup (CCOW) protocols as it communicates with and provides access to other applications.
- The GUI solution must be configured to meet DoD Information Assurance (IA) requirements, with emphasis on the following needs:
 - Supports standards for Web services that support a "plug-n-play" approach using remote portlets that service data from disparate sources supporting WSRP 2.0.
 - Provide capability for users to customize and save the view of the GUI by adding or removing portlets and features (e.g., color, layout, date range, initial view).
 - Allow registered users to personalize their view of the website by turning on, or off, portions of the webpage; or by adding or removing features based on privileges.
 - Integrate content from different sources within a portal; both client-based, and Web-based.

Objective Set 4 – AHLTA/CHCS Stabilization

The purpose of this objective is to stabilize the features in AHLTA and CHCS to improve the clinical and dental user's experience with stability, reliability and performance.

Dependencies: This objective is anticipated to be performed in parallel with Objective 5 – Theater Improvements.

Statement of Need:

- The functionality in AHLTA and CHCS should be configured to operate as loosely coupled services to reduce dependencies and create a layer of abstraction.
 - These capabilities should be exposed as discrete services that may be used in a portal framework.
- Stabilization should be achieved through the development and/or leveraging of common services (e.g., order entry, patient registration, patient administration, appointments,

scheduling, ancillary service management, results retrieval) across all EHR applications (e.g., AHLTA, Essentris). Many of the services required to replace CHCS modules have been developed. That work will be provided as GFI.

- Define, document, coordinate, manage, and verify all data/web services requirements applicable to the revised AHLTA/CHCS system. Identify, support development, document, coordinate, and verify all system interface and data/web services requirements from the revised AHLTA/CHCS system to internal and external systems. Provide traceability of all requirements and interfaces to the SRD.
- Users should be able to globally access practice management and ancillary management functions currently in local CHCS systems while maintaining the business rules. Practice management and ancillary service functions of CHCS should be able to operate from an enterprise rather than MTF-based approach using modernized loosely coupled services so that orders and results can be accomplished from MTF-to-MTF. An example is accomplishing the intent of MTF-to-MTF order portability within the DoD such as Lab Interoperability Phase 3.
- Standardized Terminology Service (e.g., Registrations, Demographics, Dispositions) must reduce the need for multiple applications to maintain the same table of data elements (e.g., ICD, CPT, Rank).
- High priority AHLTA defects that have not been addressed (APPENDIX A- EHR System Defects and SCRs) must be repaired.
 - The first tab contains the highest priority defects.
 - The second tab contains additional defects for consideration.
- High priority Ancillary services and Essentris EHR Interface and Interoperability SCRs shown in APPENDIX A- EHR System Defects and SCRs must be repaired.
- AHLTA modernization and enhancements that include a common IBM Workplace forms service should be integrated.
- The data from both Theater and Garrison must be seamlessly visible across various echelons of care within the clinical workflow.
- Capabilities in pre-production AHLTA 4.0 baseline to include but not limited to Navy Individual Medical Readiness (IMR), Duty Not Involving/Including Flying (DNIF), Personnel Reliability Program (PRP), Injury Cause Coding (ICC), DoD Profile and integrated document review module should be integrated/simplified in order to simplify review of historical documents, artifacts, encounters, and ancillary services.
- The current architectural components, such as the interface engines, Front End Processors (FEP), egate, Clinical Data Repository (CDR) sync server, enhanced Local Cache Server (LCS) capabilities and others should be reengineered using modern industry best practices and replaced with sufficient performance capacity to meet current and projected demands.
- The current AHLTA IMR should be replaced with links to the service IMR systems.
- The current User Identity Management (UIDM) must be unified by replacing current UIDM products such as Snareworks and modifying all current DHMS EHR applications to use new enterprise identity management product J-AD from TIMPO.
- Master Data Management (MDM) practices must be updated to leverage Master Patient Index/Patient identity management from DEERS (DMDC) and MDM products.
- One of the business areas heavily impacted by the removal of the printed SSN from the face of the DoD ID and Common Access Cards is the Military Health System (MHS). The printing of the DoD Number (also known as the EDI PI and Patient ID) will allow for the MHS, through CHCS, to properly identify patients for medical encounters and eligibility inquiries. CHCS and AHLTA already store the DoD EDI PI. CHCS and AHLTA are required to create the ability to find/query for a patient using the DoD EDI

PI. To search internally by the DoD EDI PI, CHCS and AHLTA must change the existing DoD EDI PI field from a text field to a searchable field. CHCS and AHLTA must update all screens where the SSN currently appears to display the DoD EDI PI. In addition, CHCS is required to utilize DMDC's Patient Add Service, Add Registry Query, and Add Registry Update. The technical specifications are depicted in APPENDIX L-Technical Specification for Patient Registration Service.

- The DEERS Registry Service should be modified to allow for CHCS to query using the DoD EDI. The registry query will include an individual and a family option so that a child could be found using a parent's ID card.
- For CHCS sites currently utilizing the DoD ID card bar code technology, the DoD EDI PI will be returned on the swipe thereby offering another method to identify patients for medical encounters and eligibility inquiries.
- System dependencies should be reengineered so that essential capabilities can still be provided when other system components are not available. For example, a provider can still document care if the orders management system is not available. In an extreme example, the system can operate offline if the network connection is severed then re-synchronize and continue operations in an online mode.
- Repair newborn metabolic screening and the registry functionality so that the capability operates with clinical best practices.
- A federated computing framework should overcome the performance and availability limitations of the current single CDR and CHCS/LCS architecture.
- The client-based PKC coupler should be removed and be replaced with integrated, web-enabled questionnaires.
- Automate software updates should be provided as a service to reduce the need for administrator intervention (to include file updates e.g. ICD9 and CPT codes).
- The current AHLTA immunization capability must be replaced with the Air Force Complete Immunization Tracking Application (AFCITA) immunization model upon the completion of its development (estimated August 2010) and delivered as GFI.
- Client software must be optimized so that it can make best use of a 64 bit environment for virtualization.
- COTS components such as Medcin, 3M and Oracle must be the current version and the use of modified COTS must be reduced.

Objective Set 5 – Theater Improvements

This objective is to enhance the functionality of the Theater suite by adding desired AHLTA-Theater, the Theater Medical Information Program (TMIP) CHCS Cache (TC2), and TMIP Framework functionality. The new AHLTA-Theater functionality should increase compatibility with TC2 and AHLTA-Theater and address existing defects. TC2 capability must be enhanced by adding bidirectional Picture Archiving and Communications System (PACS) support and should interface with lab instruments. The TMIP framework should be enhanced to address current shortfalls in functionality such as guaranteed message delivery and secure socket layer support. This should help bridge the gap between the Sustaining Base software baseline and the Theater.

Dependencies: This objective is anticipated to be performed in parallel with Objective 4 – AHLTA/CHCS Stabilization.

Statement of Need:

- Overarching Improvements

- AHLTA-Theater issues depicted in APPENDIX A-EHR System Defects and SCRs must be repaired.
- TC2 issues depicted in APPENDIX A-EHR System Defects and SCRs must be repaired.
- Leverage the enterprise duplicate patient record solution that will be provided as GFI to reduce duplicate patient record instances across Theater.
- Extend Garrison AHLTA/CHCS capabilities in a common baseline to the Theater of Operations to provide a “train as you fight” user experience in the system. The Theater based system must have the same look, feel and baseline functionality however operate in an austere environment with limited computing, communication and system administration resources.
- Ensure all relevant patient data captured in Theater is made part of the lifelong electronic health record as described in the Theater Medical Data Integration (TMDI) section in APPENDIX ~~M~~ – Government Furnished Information. The data from both Theater and Garrison must be seamlessly visible across various echelons of care within the clinical workflow for health history viewing.
- Add Common Access Card (CAC) capability to users as an additional logon option.
- A Standardized Terminology Service (e.g., registrations, demographics, dispositions) must be provided to reduce the need for multiple data dictionaries (e.g., ICD, CPT, Rank).
- Must enhance interface between AHLTA-Theater and TC2 to address:
 - Order entry and results retrieval between AHLTA-Theater and TC2,
 - Reviewing TC2 inpatient notes within AHLTA-Theater, and
 - Leverage the use of the EDI_PN_ID as the unique identifier for person identity between AHLTA-Theater and TC2.
- AHLTA-Theater Capability
 - IBM Work Place Forms – Incorporating Sustaining Base solutions for forms management must provide data transportability between Sustaining Base and Theater (e.g., forms created in Sustaining Base must be usable in Theater).
 - Should support Service-specific eForms.
 - Initiatives for accommodating Personnel Reliability Programs (PRPs) and DNIF status must be supported.
 - The current Very Important People (VIP) functionality in the system must not be altered.
 - Implement the DoD extensions for Injury Cause Coding for use in the patient encounter process.
 - The Theater EHR solution should enable adoption of Sustaining Base dental enhancements.
 - Leverage the Web module provided as GFI to provide:
 - Reach back to comprehensive health history,
 - Full access to HAIMS, NCAT, Traumatic Brain Injury (TBI)/BH, the Theater Medical Data Store (TMDS) and Immunizations, and
 - Web-Enabled Health Assessment Review Tool (HART) solution.
 - The Sustaining Base “copy-forward” capability should be integrated in the Theater solution.
 - Provide a configuration utility to ease the setup and management of the system.
 - The database in Theater solutions should facilitate simplified deployment, distribution and administration and minimize hardware requirements.
 - AHLTA-Theater issues depicted in APPENDIX A-EHR System Defects and SCRs must be repaired.
- Implement new TC2 capabilities provided as GFI

Deleted: 1

- Bidirectional PACS interface
- Order-entry and results retrieval
- Nursing orders messaging
- EDI_PN_ID
- Lab equipment interface
- TC2 issues depicted in APPENDIX A-EHR System Defects and SCRs must be repaired.
- Provide a capability for TC2 orders and results to be portable between Theater/Theater and Theater/Sustaining Base hospitals.
- TMIP Communication Framework
 - Should provide a more robust and technically advanced application for communicating between Theater products using a SOA approach including:
 - Communications for Austere Environments
 - Scalable
 - Dashboard
 - Configuration utility
 - Lightweight application
 - Bidirectional messaging capability
 - Backward operability with message format
 - Secure socket layer capability
 - Navy proxy support
 - Guaranteed message delivery
 - Message confirmation
 - Sort and filter message configuration
 - Capability for dynamic message routing
 - Should provide intelligent transfer for large files with automatic recovery of the data transfer, without restarting the transfer of data if network communication is disrupted.
 - Logging, debugging and reporting capabilities should be enhanced to include failure notification messaging.
 - TMIP framework issues depicted in APPENDIX A-EHR System Defects and SCRs should be repaired.

Objective Set 6 – Content Management System (CMS) ((Optional Task and should be priced seperately)

This objective shall acquire, configure, and implement enterprise CMS containing EHR system-related information (non-patient related) to be hosted in a government selected portal framework. This system can be accessed by the user from the GUI framework depicted above. Users should be able to access the portal to provide and/or obtain EHR system information, multimedia content in various formats including articles, discussion boards, blogs, Wiki and help files. Approved users of the CMS should be able to disseminate information and collaborate in developing the content for the larger healthcare community.

Dependencies: None.

Statement of Need:

- A CMS should be acquired, configured and deployed to be made available through the enterprise GUI as a portlet providing access to EHR information, and also as a standalone EHR informational website. The centrally managed capability must not include any patient information, patient-related information or patient record information.

- This capability is intended for EHR system related information such as news article, system message (e.g., downtime), help files, discussion boards/forums and manuals (e.g., Wikipedia), blogging and commentary.
- Approved users can directly create and edit content without the assistance of a traditional web master or advance information technology skills.
- The EHR system user community should have the capability to collaboratively review, index, search, and publish non patient care related forms of digital media (e.g., images, audio, video) and electronic text.

Objective Set 7 – Operations and Maintenance Activities

A sustainment option period may be ordered immediately following delivery and deployment of a substantial portion of the FHCC NC functionality, and will continue throughout the end of the contract. This objective includes tier 2 and tier 3 support for trouble tickets, and reporting on status, availability and usage of the GUI, ESB and the patient registration portlet. Additional ESB activities include maintenance of the common repositories/services such as the common data tables, web services directory, and translation services to implement changes as required. Additional O&M activities for the patient registration portlet include analysis and implementation of approved changes and provisioning the portlet to other applications/portals.

Dependencies: None.

Statement of Need:

O&M activities for the GUI should include:

- Maintenance activities of core capabilities provided solely by the GUI application,
- Tier 3 support for trouble tickets on core capabilities solely by the GUI application,
- Tier 2 for portlets (with the understanding that the provider of the portlet is Tier 3 meaning they work with the vendor to support any enhancement requirements to function through the GUI),
- Support for provisioning of new portlets to include developmental support and tier 2 support for portlet issues as above,
- Weekly availability and usage reporting, and
- Daily status reporting and a notification process for reporting up to DHIMS.

O&M activities for the ESB should include:

- Same status and reporting as above to include transaction statistics, hourly message failure tracking and trouble shooting and a notification process for reporting up to DHIMS,
- Same tier support above for messages,
- Table maintenance for common data tables (DMIS ID, UIC, Zip Code, etc),
- Web services directory maintenance,
- Update translation services, if needed, for new interfaces.

O&M activities for the Patient Registration Portlet should include:

- Tiered support and reporting as above to include tier 3 support for GUI issues,
- Support for SCR validation and enhancements whether related to MHS GUI or any other GUI that must use the portlet,

Support for provisioning portlet to new applications/portals

3.0 INSPECTION AND ACCEPTANCE

The COR specified in the COR appointment letter is responsible for inspection and acceptance of all incoming shipments, documents, and services.

3.1 Acceptance Criteria

Certification by the Government of satisfactory services provided is contingent upon the Contractor performing in accordance with the performance standards contained in the Performance Requirements Summary Matrix (Section 6.8.2) and all terms and conditions of this order, including all modifications.

3.2 Contractor Payment Processing

The Contractor is responsible for properly preparing, and forwarding to the appropriate Government official, the invoice and receiving report or Public Voucher for payment. The Contractor shall attach back up information to receiving reports for direct labor and Other Direct Costs (ODCs). Direct labor backup information shall reflect the person's name, job title and quantity of hours worked for each pay period at a minimum. Backup information for ODCs shall list all elements of costs, such as travel breakout backup, including itinerary, dates of travel, name of employees traveling plus per diem costs shall accompany the receiving report. All ODCs exceeding \$3,000 requires that the Contractor conduct appropriate competition.

Deleted: When the direct submission process is used, the Contractor shall submit the invoice or public voucher directly to the payment office and concurrently submit a copy to the COR

Deleted:

3.3 PROCEDURES FOR PAYMENT

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

- (1) The end of the invoiced month (*for services*) or
- (2) The end of the month in which the products (*commodities*) or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Cost type contracts:

The contractor shall invoice monthly on the basis of cost incurred for the CPFF Labor CLINs. All hours and costs shall be reported by WBS element in accordance with the approved submitted WBS numbering system and definitions. Invoices shall list the contractor employee and shall be provided for the current billing month in total from project inception to date. The contractor shall provide the invoice data on separate worksheets in spreadsheet form with the following detailed information. The invoice shall include the period of performance covered by the invoice and the WBS numbers and titles. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Employee name (current and past employees)
- Employee company labor category
- Employee Millennia labor category and Associated Skill Level Number
- Actual Hours worked during the monthly billing period and total cumulative hours worked
- Billing rate

Formatted: Font: 11 pt

Deleted: CLIN

Formatted: Font: 11 pt

Deleted:

Deleted: and

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Deleted: ,

Deleted: and

Deleted: CLIN

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Payment of fixed fee will be on an hourly basis determined at time of award based on total proposed fee and total level of effort proposed. The fee is fixed and will not be reflected as a percentage of cost.

Formatted: Indent: Left: 0.5"

▲ All cost presentations provided by the contractor shall also include Overhead Charges, and General and Administrative Charges clearly shown both as a percentage and total dollars.

Formatted: Font: 11 pt

▲ The Government reserves the right to modify invoicing requirements at its discretion. The contractor shall comply with any revised invoicing requirements at no additional cost to the Government.

Formatted: Font: 11 pt

The contractor may invoice only for the hours, travel, tools, and ODCs, ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum:

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Training Itemized by Individual and Purpose (if applicable) billed to ODC CLIN
8. Support Items listed by Specific Item and Amount (if applicable) billed to ODC or Tools CLIN as appropriate.

For Labor Hour and Time and Material orders/contracts each invoice *shall* show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Posting Acceptance Documents: Invoices shall initially be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the CR. Included with the invoice will be all backup documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following options in accepting and certifying services;

- a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. **NOTE: The Government's preference is that receiving agency's acceptance is conducted electronically.**
- b. On Paper Copy: The client agency may accept and certify services by providing written acceptance with the signature of the authorized client representative and the date of acceptance.

Electronic and/or written acceptance of the invoice by the CR is considered concurrence and acceptance of services. Regardless, of the method of acceptance the contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. (Written acceptances will be posted as an attachment along with any other supporting documentation.) After acceptance of the invoice by the CR, the Contractor shall submit a proper invoice to GSA Finance not later than five (5) workdays after acceptance by the Government of the product, service, and/or cost item. In the absence of Government acceptance within thirty (30) days, the contractor shall submit an invoice.

Note: The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoice submitted. Although this acceptance may occur in two ways, electronically or in paper copy, at least shall be obtained prior to the approval of payment. In order to expedite payment, it is *strongly recommended* that the contractor continue to include the receiving agency's WRITTEN acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

Note: If any invoice is received without the required documentation and, (A) the customer's *signed* written acceptance OR (B) the customer's electronic acceptance, the invoice *shall* be rejected in whole or in part as determined by the Government.

Posting Invoice Documents: Contractors shall submit invoices to GSA Finance for payment, after acceptance has been processed in GSA's electronic Web-Based Order Processing System, currently ITSS. The contractor has the option of posting the invoice on GSA's Ft. Worth web site, www.finance.gsa.gov/defaultexternal.asp or mail to the address shown on BLOCK 24 of the GSA FORM 300. **NOTE: Only use one method of submission, web site or regular U.S. mail, but not both.**

U.S. Mailing Address:
GSA Finance Center
P.O. Box 17181
Fort Worth, TX 76102-0114

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

9. GSA Task Order Number
10. Task Order ACT Number
11. Remittance Address
12. Period of Performance for Billing Period
13. Point of Contact and Phone Number
14. Invoice Amount
15. Skill Level Name and Associated Skill Level Number
16. Actual Hours Worked During the Billing Period
17. Travel Itemized by Individual and Trip (if applicable)
18. Training Itemized by Individual and Purpose (if applicable)
19. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary*.

Close-out Procedures.

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period [pending finalization of indirect costs](#). After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment [pending finalization of indirect costs](#). ▼

Deleted:

4.0 DELIVERABLES

4.1 Delivery Address

All deliverables shall be submitted to the COR, and to the Fiscal, Project, and Technical Support contacts who shall be identified by the COR. The Contractor shall also submit all deliverables to the Contract Deliverables Requirements List (CDRL) Support Center and the Configuration Management (CM) Library Support Center at the following addresses:

Organization: DHIMS
ATTN: CDRL Support Center
Address: 5109 Leesburg Pike, Suite 800
Falls Church, VA 22041-3206
Phone Number: (703) 933-3761 ext. 305
Fax Number: (703) 998-0198
Email Address: DHIMS.CM.CDRL@tma.osd.mil

Organization: DHIMS
ATTN: CM Library Support Center
Address: 5109 Leesburg Pike, Suite 800
Falls Church, VA 22041-3206
Phone Number: (703) 933-3761 ext. 305
Fax Number: (703) 998-0198
Email Address: DHIMS.CM.product@tma.osd.mil

4.2 Method Of Delivery

Electronic copies shall be delivered using Microsoft Office suite of tools (for example, MS WORD, MS EXCEL, MS POWERPOINT, MS PROJECT, or MS ACCESS format), unless otherwise specified by the COR. Electronic submission shall be made via email, unless otherwise agreed to by the COR.

4.3 Government Acceptance Period

The COR will have ten (10) workdays to review draft deliverables and make comments. The Contractor shall have five (5) workdays to make corrections. Upon receipt of the final deliverables, the COR will have two (2) workdays for final review prior to acceptance or providing documented reasons for non-acceptance. Should the Government fail to complete the review within the review period the deliverable will become acceptable by default, unless prior to the expiration of the ten (10) work days the Government notifies the Contractor in writing to the contrary. The final submission should be deemed approved if the Government has not rejected it in 30 days.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have five (5) workdays to correct the rejected deliverable and return it per delivery instructions.

4.4 Criteria for Deliverable Acceptance

Milestone Chart/Deliverable Schedule:

Reviewer	Management Report Deliverables	Description	Delivery Time
TMA PM	Final SOW submittal	Submittal of the Statement of Work in final draft form incorporating any change requests and or post award clarifications	10 working days following task order award.
TMA PM	Complete technical solution (to include all source and executable software code)	Objective 1 - FHCC technical solution - DoD and VA integrated information system at the CAPT James A. Lovell Federal Health Care Center (FHCC NC)	
TMA PM/ GSA COTR	Revised schedule and GANTT chart	Updates to the schedule management plan and Gantt chart are anticipated as development uncertainties become known.	As needed. Contractor shall notify GSA COTR and CO immediately upon discovery of schedule changes and impacts.
Management	Finalized Schedule baseline	Submit the finalized schedule baseline which incorporating any change request	10 day after award
TMA PM	All portlets and other components associated with the FHCC technical solution	Objective 3 – GUI provides a common web user interface using the government furnished portal framework	
TMA PM	Training materials	Provide a training outline and associated training material to the TMA Program Manager for approval.	5 working days prior to the start of training.
Management	Test and Acceptance Checklist for software functionality	The Contractor or his designee shall develop and submit a complete Test and Acceptance Checklist based on there proposed solution.	Upon completion of each objective

TMA PM/ GSA COTR	Final Test and Acceptance Report	The Contractor shall perform a complete acceptance test. The Contractor shall correct any deficiencies prior to the director brief.	Upon each installation completion
Management	Mgmt Report Deliverables: Contract Performance Report (CPR) Formats 1, 2, 3, 4, & 5	The Contractor shall provide CPR Format 1 data (organized by WBS), CPR Format 2 data (organized by contractor's organization), CPR Format 3 data (budget baseline plan), CPR Format 4 data (staffing forecasts), and CPR Format 5 data (cost and schedule variance narrative report).. Link to the DID: http://www.acq.osd.mil/pm/currentpolicy/cpr_cfsr/CPR%20Final%203-30-05.pdf	Monthly, NLT 15 calendar days after end of previous month

5.0 CONTRACT ADMINISTRATION DATA

5.1 Place of Performance

The Contractor shall perform primary activity at the Contractor's facility with other locations (Government and Contractor test laboratories) as determined by the TMA Program Manager.

5.2 Period of Performance

The period of performance shall be for one (1) twelve-month base period and three (3) twelve-month option periods.

5.3 Other Direct Costs (ODCs)

Travel

Occasional travel may be required to the following locations; VA and DOD FHCC facilities in Chicago, the primary data center Montgomery, Alabama, Maxwell- Gunter AFB, AL, and various Test Environment/COOP facilities within the Mid Atlantic Region. The TMA PM will approve all travel requirements/requests before the travel is to begin. The Contractor shall be entitled to recovery of reasonable transportation costs incurred for employees. Reimbursement of travel will be accomplished when the Contractor submits an invoice for travel along with supporting documentation (receipts as required by Federal Travel Regulations). Expenses for subsistence and lodging will be reimbursed to the Contractor only to the extent where overnight stay is necessary and authorized by the Federal Travel Regulation in effect at the time of the stay for this specific location. All travel and per diem expenses will be reimbursed in accordance with the Federal Travel Regulations. Federal Travel Regulations require receipts for travel expenditures of \$75.00 or more. The receipts shall be submitted with invoices.

Travel Outside of the U.S.

~~There is no requirement for Travel outside of the U.S.~~

Other Direct Costs (ODCs)

ODCs shall be billed on a cost reimbursable basis. Costs are defined as the purchase price of materials or service plus General and Administrative charges (G&A) or material and handling charges (M&H). G&A or M&H charges received by the Contractor are subject to periodic Government conducted DCAA audits and to adjustment as a result of the final contract closeout audit conducted by DCAA. Profit/fee on ODCs other than subcontracting are prohibited. When subcontracting is included as part of the Contractor's technical approach on individual task orders, a fixed profit/fee will be allowable, but shall not exceed the fixed fee contained in the final basic contract CPFF award.

All ODCs shall be fully supported in compliance with all competition requirements of the FAR, specifically Part 31.

5.4 Order Administration and Points of Contact:

All order administration functions will be retained by the GSA Contracting Officer. All inquiries and correspondence relative to the administration of the order shall be addressed to the GSA COTR and copied to the GSA Contracting Officer.

GSA COTR / Information Technology Manager

Deleted: This order includes activity that may require Contractor travel to destinations outside of the United States. The Contractor shall ensure that assigned participants allow sufficient lead-time to obtain valid passports, country clearances, and immunizations to support project activities. All travel outside of the U.S. required under this tasking shall be laid out in the travel matrix above.

Deleted: 1. All ODCs shall be reported as stated in the Procurement of Hardware, Software, Equipment and Materials Section 2.2.3.1, as well as the Monthly Progress Report Section 2.1.2.2.

Ibrahiim Kent
IT Specialist, GSA FAS
Voice (215) 446-5825
Fax: (215) 814-6119
Ibrahiim.Kent@gsa.gov

GSA Contracting Officer
Debra Stuart
Contracting Officer, GSA FAS
Voice: (215) 446-5817
Fax: (215) 829-2817
Cell: (609) 668-2482
Debra.Stuart@gsa.gov

GSA Contract Specialist
Jacqueline T. Stanback
Contracting Officer, GSA FAS
(215) 446-5839 phone
Jacqueline.Stanback@gsa.gov

TMA Program Manager
MAJ Frank Tucker, USA
Director, System Development
Voice: (703) 998-6900 x1119
Fax: (703) 379-0604

TMA Contracts Manager
Chris Kuhn
Deputy Director, DHIMS Resource Management
Voice: (703) 575-2756
Fax: (703) 575-2733

TMA Acquisition Manager
Aaron Street
Voice: (703) 681-1143
Fax: (703) 681-6036
Aaron.Street@tma.osd mil

6.0 OTHER TERMS, CONDITIONS, AND PROVISIONS

6.1 Non-Disclosure / Non-Use Agreement

The Contractor shall ensure that the Non-Disclosure Statement is signed by all staff assigned to or performing on this Task order before performing any work, including all sub-contractors and consultants. The Non-Disclosure / Non-Use statement will be cosigned by a corporate official (Contractor Task Manager or higher). The Contractor shall also ensure that all staff understand and adhere to the terms of the non-disclosure statement, protecting the procurement sensitive information of the Government and the proprietary information of other Contractors. Assignment of staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor. The Non – Disclosure Statement shall be provided post award.

Deleted: (Appendix A)

Deleted: C

6.2 Information Assurance

General Security Requirements

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data. As a minimum, this shall include provisions for personnel security, electronic security and physical security as listed in the sections that follow:

Personnel Security

The Contractor shall comply with DoD Directive 8500.1, "Information Assurance (IA);" DoD Instruction 8500.2, "Information Assurance (IA) Implementation;" DoD Directive 5400.11, "DoD Privacy Program;" DoD 6025.18-R, "DoD Health Information Privacy Regulation;" and DoD 5200.2-R, "Personnel Security Program Requirements."

Contractor responsibilities for ensuring personnel security include, but are not limited to, meeting the following requirements:

Follow the TMA Privacy Office guidelines for submittal of Automated Data

Processor/Information Technology (ADP/IT) security clearances and ensure all Contractor personnel are designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III where their duties meet the criteria of the position sensitivity designations. Contact the TMA Privacy Office for guidance on the appropriate ADP/IT levels for personnel on the contract. The TMA Privacy Office procedures for personnel security are listed on the following website:

<http://www.tricare.osd.mil/tmaprivacy/personnel-security.cfm>.

Initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to MHS Sensitive Information (SI).

Immediately report to the TMA Privacy Office and deny access to any automated information system (AIS), network, or MHS SI information if a Contractor employee filling a sensitive position receives an unfavorable adjudication, if information that would result in an unfavorable adjudication becomes available, or if directed to do so by the appropriate Government representative for security reasons.

Ensure that all Contractor personnel receive information assurance (IA) training before being granted access to DoD AISs/networks, and/or MHS SI information.

Electronic Security

Contractor Information Systems (IS)/networks that are involved in the operation of systems in support of the DoD MHS shall operate in accordance with controlling laws, regulations, and DoD policy.

Contractors designing, developing or operating DoD ISs shall comply with the requirements of the DoD Information Assurance (IA) program as promulgated in DoDIA 8500.2IA Implementation, 6 February 2003.

Certification & Accreditation (C&A) requirements as promulgated in DoDI 8510.01 apply to all DoD and Contractor's IS/networks that receive, process, display, store or transmit DoD information. The Contractor shall comply with the C&A process for safeguarding SI. Certification is the determination of the appropriate level of protection required for IS/networks. Certification also includes a comprehensive evaluation of the technical and non-technical security features and countermeasures required for each system/network.

Accreditation is the formal approval by the Government to operate the Contractor's IS/networks in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, accreditation allows IS/networks to operate within the given operational environment with stated interconnections; and with appropriate level of protection for the specified period.

The Contractor shall comply with C&A requirements, as specified by the Government, that meet appropriate DoD Information Assurance requirements. The C&A requirements shall be met before the Contractor's system is authorized to access DoD data or interconnect with any DoD IS/network that receives, processes, stores, displays or transmits DoD data. The Contractor shall initiate the C&A process by providing the Contracting Officer, within 60 days following contract award, the required documentation necessary to receive an Approval to Operate (ATO). The Contractor shall make its IS/networks available for testing, and initiate the C&A testing four months (120 days) in advance of accessing DoD data or interconnecting with DoD IS/networks. The Contractor shall ensure the proper Contractor support staff is available to participate in all phases of the C&A process. This include, but is not limited to:

- Attending and supporting C&A meetings with the Government
- Supporting/conducting the vulnerability mitigation process
- Supporting the C&A Team during system security testing

Contractors must confirm that their IS/networks are locked down prior to initiating testing.

- Confirmation of system lock down shall be agreed upon during the definition of the C&A boundary and be signed and documented as part of the System Security Authorization Agreement (SSAA)
- Locking down the system means that there shall be no changes made to the configuration of the system (within the C&A boundary) during the C&A process

Any re-configuration or change in the system during the C&A testing process will require a re-baselining of the system and documentation of system changes.

Vulnerabilities that have been identified by the Government as "must-fix" issues during C&A process must be mitigated according to the timeline identified by the Government Representative. C&A checklists are provided for complying DoD C&A requirements. Reference material and C&A tools may be obtained at: <http://iase.disa.mil/ditscap>.

A request for a waiver to the C&A requirements may be submitted for temporary testing and other usual circumstances. A waiver request must be submitted, in writing, to the Designated Accrediting Authority (DAA). The request must include mitigation strategies that ensure adequate protection measures and security controls are in place (for example: air gapping a testing network).

Information Assurance Vulnerability Management (IAVM)

The Contractor shall implement an information assurance vulnerability management program. The DoD IAVM program provides electronic security protections against known threats and vulnerabilities. The IAVM program requires the registration of DoD IS assets in the DoD Vulnerability Management System (VMS), which allows for the timely dissemination of critical vulnerability information. It also assists in the documentation and tracking of compliance, providing increased electronic security to MHS systems. As part of the program, the Contractor shall provide a primary and secondary point of contact in the VMS and to the MHS Information Assurance Vulnerability Alert (IAVA) Monitor. The point of contact shall provide, upon receipt of a vulnerability message, an acknowledgment of receipt via the VMS. The contractor shall thoroughly test all mitigations for the vulnerability, and upon applying the mitigation to the system, report compliance in the VMS. Receipt and compliance messages to the Government shall occur within the stipulated time window, as stated in the vulnerability message or in the VMS.

The Contractor shall ensure DoD IS assets that are under development are registered in the VMS and have all applicable electronic patches installed for the system (1) when the system is delivered to the Government, or (2) if the DoD IS assets are used to store or process Government data prior to delivery (such as when being used in testing and development).

Guidance regarding the requirement for IAVM is contained in the DoD Information Assurance Vulnerability Alert (IAVA) December 30, 1999 memorandum and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 (Appendix A to Enclosure B) provides additional reference information. Implementation is addressed in the Defense Information Systems Agency (DISA) IAVA Process Handbook, Version 2.1, June 11, 2002. An asset is any device on any DoD-owned, controlled or contracted IS or network, to include (but not limited to) workstations, servers, routing devices (routers, switches, firewalls), networked peripherals (e.g., network printers, portable electronic devices) and controlled interfaces (e.g., guards). A device is considered a node on a network if it has its own network identification (internet protocol (IP) and/or media access control address). The Defense Information System Agency's (DISA) VMS web enabled application is used to disseminate IA Vas Information Assurance Vulnerability Bulletins (IA VBs), and Information Assurance Technical Advisories down to the System Administrator (SA) and applicable personnel throughout the chain of command.

The Contractor shall maintain any development environments in accordance with TMA Information Assurance IA best practices and operational requirements. During product development for the Government, the Contractor shall ensure that all IA mitigation strategies have been applied to the development environment prior to any Government data being loaded onto any assets or software for testing or delivery.

IA mitigation strategies include security updates, service packs, and changes to operating procedures as physical and cyber vulnerabilities are detected. Operating system, routers, servers, development platforms and the application being delivered to the Government shall be in compliance with all known applicable Department of Defense Computer Emergency Response Team (DoD-CERT) Alert, Bulletin, and Technical Advisory Notices published during the past 36

months.

Disposing of Electronic Media

Contractors shall follow the DoD standards, procedures, and use approved products to dispose of unclassified hard drives and other electronic media, as appropriate, in accordance with DoD Memorandum "Disposition of Unclassified Computer Hard Drives," June 4, 2001. Contractors are required to also follow DoD guidance on sanitization of other internal and external media components in DODI 8500.2 "Information Assurance (IA) Implementation," 6 Feb 2003 (see PECS-1 in enclosure 4 Attachment 5) and DoD 5220.22-M "Industrial Security Program Operating Manual (NISPOM)," (Chapter 8).

Ports, Protocols, and Services. Contractors shall follow all current DoD and Defense Information Systems Agency (DISA) standards and requirements for acceptable Ports, Protocols, and Services. Any requests for exception to using the current DISA Ports, Protocols, and Services standards requires an request for exception sent through the Program Manager to the DAA.

Public Key Infrastructure and Encryption. Contractors shall follow the DoD standards, policies, and procedures related to the use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication. Where interoperable PKI is required for the exchange of unclassified information between DoD and its Contractors, industry partners shall obtain all necessary certificates. Contractors must turn over to the Government all encryption keys for deployed systems, backdoor algorithms, and procedures for their use in remote support. Contractors must provide a written report detailing all of the above, prior to task order expiration, regardless of modifications or extensions.

Information Systems (IS)/Networks Physical Security

The Contractor shall employ physical security safeguards for IS/Networks involved in processing or storage of Government Data to prevent the unauthorized access, disclosure, modification, destruction, use, etc., and to otherwise protect the confidentiality and ensure use conforms with DoD regulations. In addition, the Contractor will support a Physical Security Audit performed by the Government of the Contractor's internal information management infrastructure. The MHS Physical Security Audit Matrix is available at:
http://www.tricare.osd.mil/tmis_new/Policy/PSA_Matrix_%20012304%200930%20clean%20version.xls.

The Contractor shall correct any deficiencies identified by the Government of the Contractor's physical security posture. The Contractor shall be required to follow all requirements in the MHS Information Assurance Policy. New MHS policies will be posted to the following website:
http://www.tricare.osd.mil/tmis_new/IA.htm.

6.3 Enterprise Architecture (EA)

For a Contractor that is providing the Government with new server or workstation capability based on Microsoft Windows, LINUX or Sun Solaris x86 based platforms, the Government requires that the Contractor provide a copy of the server, as a VMware VM, in the same configuration as it would be deployed to the field with all DISA STiGs applied and software installed and functioning.

The Government requests a small document with the base configuration of the VM, to include:

- Number of virtual processors
- Memory requirements of the VM

- Number of virtual network adapters assigned to the VM
- Any special network configuration requirements
- If there are multiple Virtual Disks assigned to the VM list them and define which drive letters are assigned to each one.
- Administrative username and passwords for the VM

In addition to this short document, the VMX and VMDK files associated with the VM should be transferred via SFTP or SCP to the DHIMS lab environment.

The development guidance packet is to be included in the list of items we deliver with the SOW and there should be words that say that the vendor shall conform to the Standards listed in the "Standards Data & Technical" worksheet and shall employ the applicable technologies listed in the "Technologies" worksheet.

Deleted: attached

Deleted: (Attachment 4)

References

Architecture/Repositories

- DOD Architecture Framework Version 2.0, May 28, 2009
- DOD Information Technology Standards Registry (DISR), Version 09-1.0, March 26, 2009
- TRICARE Management Activity – Military Health System Enterprise Architecture version 5.0 or more current version

Business Transformation

- Deputy Under Secretary of Defense for Financial Management and the Deputy Under Secretary of Defense for Business Transformation Memorandum, "Release of New and Updated Department of Defense Business system Investment Review Related Guidance," April 11, 2006

General

- DODD 5000.01 Defense Acquisition System, May 12, 2003
- DODI 5000.02 Operation of the Defense Acquisition System, May 12, 2003
- DODI 5025.01 DoD Directives Program, October 28, 2007
- DOD 5500.7-R Joint Ethics Regulation, Current version
- DOD 6015.1-M Glossary of Healthcare Terminology, January 13, 1999
- DODD 8000.01 Management of the DoD Information Enterprise, February 10, 2009
- Joint Vision 2020, May 20, 2000
- Electronic Industry Association 548, Electronic Design Interchange (Format) (EDIF), Version 400, August 1996
- Office of Management and Budget (OMB) Circular NO. A-130: Management of Federal Information Resources, November 28, 2000
- Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger Cohen Act of 1996 (Public Law 104-106)," June 2, 1997
- Assistant Secretary of Defense (Health Affairs) Memo "Improving Medical Record Coding at Military Treatment Facilities," August 20, 2003

Global Information Grid(GIG)/Net-Centricity

- Global Information Grid (GIG) Capstone Requirements Document, 5 JROCM 134-01, August 30, 2001
- Global Information Grid (GIG) Architecture Version 2.0, August 2003

- DoD CIO Memorandum, “Global Information Grid Enterprise Services (GIG ES): Transforming to a Net-Centric Environment—President’s Budget FY 2006-2011,” July 30, 2004
- DOD Deputy CIO, Information Management Memorandum, “Department of Defense (DoD) Net-Centric Data Strategy: Accessibility – Posting Data to Shared Spaces: Memoranda Coordination Request—Action Memorandum”, November 14, 2003
- DOD CIO Memo “Department of Defense (DoD) Net-Centric Data Strategy: Visibility – Tagging and Advertising Data Assets with Discovery Metadata,” October 23, 2003
- DOD CIO Memo “DOD Net-Centric Data Strategy: Visibility – Advertising Data Assets with Discovery Metadata,” May 30, 2003
- DOD Net-Centric Data Strategy, May 9, 2003
- DOD CIO Memo “Department of Defense (DoD) Net-Centric Data Management Strategy: Metadata Registration,” April 3, 2003
- DODD 8320.2 Data Sharing in a Net-Centric Department of Defense, December 2, 2004
- DOD Guidance 8320.02-G Guidance for Implementing Net-Centric Data Sharing, April 12, 2006

Joint Capabilities Integration and Development

- CJCSI 3170.01F Joint Capabilities Integration and Development, May 1, 2007
- CJCSM 3170.01C May 1, 2007

Laws

- Federal Information Security Management Act of 2002
- Public Law 104-113: National Technology Transfer and Advancement Act of 1995. 104th Congress, March 7, 1996
- Public Law 104-106: Clinger-Cohen Act of 1996, February 10, 1996
- Health Insurance Portability and Accountability Act, 1996
- Public Law 93-579: Privacy Act of 1974

Metadata

- DOD Director, Information Management Memorandum, “Migration of DoD Data Dictionary System (DDDS) Data Assets --- DoD Metadata Registry and Clearing House”, November 24, 2003
- Draft DOD Discovery Metadata Standard (DDMS), June 2, 2003

Security/Information Assurance/Technology

- DODD 4630.05 Interoperability and Supportability of Information Technology (IT) and National Security systems (NSS), May 5, 2004
- DODD 8100.02, Use of Commercial Wireless Devices and Services in the DOD Global Information Grid, April 14, 2004
- DODD 8500.01, Information Assurance, October 24, 2002
- DODI 8500.2, Information Assurance (IA) Implementation, February 6, 2003
- DODI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security systems (NSS), June 30, 2004
- Interim DOD Certification and Accreditation Process Guidance, July 6, 2006.
- DOD CIO Memo “Internet Protocol Version,” August 16, 2005
- CJCSI 6212.01D Interoperability and Supportability of Information Technology and National Security systems (NSS), March 8, 2006

- NSTISSP No. 11, 4 National Policy Governing Information Assurance and Information Assurance Enabled Information Technology Products, January 2000

Reference URLs

- <http://www.whitehouse.gov/omb/e-gov/fea> (Federal Enterprise Architecture Security and Privacy Profile)
- <https://disronline.disa.mil/DISR/index.jsp> (A Common Access Card is required)
- <http://ipv6.disa.mil> (A Common Access Card is required)
- <http://www.defenselink.mil/cio-nii/policy/eas.shtml>
- <http://www.bta.mil/index.html>
- <http://www.dod.mil/pubs>

MHS Enterprise Architecture Requirements -- General

The Contractor shall adhere to goals, standards, constraints, guidelines, products architectural products, and processes established and approved by the MHS Enterprise Architecture Board, Chief Enterprise Architect, subordinate boards or Integrated Product Teams, or higher levels of authority. These products are available as GFI from the MHS Chief Architect via DHIMS architecture team.

The Contractor shall ensure that products and services (deliverables) are aligned and compliant with the current MHS Strategic Plan, MHS IM/IT Strategic Plan and Principles, MHS Enterprise Architecture, DoD Architectural Framework, Global Information Grid Architecture, DoD Business Enterprise Architecture, the Federal Enterprise Architecture Framework (OMB Reference Models), and when requested with Services' Operational Architectures (e.g. AMEDD).. These products are available as GFI from the MHS Chief Architect via DHIMS architecture team.

The Contractor shall employ strategies, technical solutions and project plans that support the DoD Net-Centric service oriented architectures.

The DoDAF v2.0 defines a common approach for DoD architecture description development, presentation, and integration. The DoDAF v2.0 is a net-centric update to the framework which provides a common approach to DoD net-centric architecture development and includes guidance to programs, managers, and architects who are developing systems that operate in the NCE as mandated by DoD CIO policies, guidance, and instruction. The net-centric update of DoDAF v2.0 leverages the previous DoDAF versions to describe three types of architectures: Traditional, Net-Centric, and Hybrid (a mix of traditional and net-centric). The Contractor should refer to the most recent DHIMS Enterprise Architecture and may consult with the DHIMS PMO as needed. The deliverables shall be importable into the DHIMS Enterprise Architecture Repository.

Accordingly, the Contractor shall:

- Comply with the most current version of the DoDAF
- Provide appropriate DoDAF Views as determined by the Program Office (All Views, Operational Views, Systems Views, and Technical Standards Views)
- Comply with the DoD Discovery Metadata Specification (DDMS)
- Provide all applicable Operational Views, System Views, Technical Views, and All Views relevant to the design and implementation of the solution illustrated below in the DoDAF v2.0 or the latest version. These artifacts shall be delivered in such a way to make them easily importable into System Architect DoDAF (C4ISR) in the current version used at MHS.
- The Contractor shall demonstrate the SOA capabilities of the system to:
 - Use secure web services

- Integrate with web services registries using UDDI
- Provide or bind to web services that comply with SOAP
- Develop testable web services for deployment on multiple web services platforms (e.g., IBM Websphere, Weblogic, net, JBOSS/Open Source)
- Integrate with multiple messaging protocols or messaging queues
- Use web services extensions (e.g., WS-BPEL, WS-Security) with additional integration of systems (e.g., Oracle BPEL Engine) into the architecture
- The Contractor shall provide the SOA Service Repository and Service Registry of the system (Deliverable xx) upon delivery of the final product. The goals of the Service Repository are to promote asset reuse and eliminate redundancies by increasing visibility of services, applications and processes, link software assets to business objectives, enable governance and policy management across the SOA lifecycle, and automate the process of recording metadata. The Service Registry will serve as the index-of-record for all deployed services within the enterprise and the business policies that affect the runtime behavior of those services. The Service Registry will free the client from static endpoint references, enforce runtime policies, and automatically notify service consumers of changes.

MHS Enterprise Architecture Requirements -- Special Requirements

The Contractor shall assist the Program Management Office in completing the MHS Net-Centric Check List in support of the Department of Defense (DoD) joint interoperability, net-centric concepts and enterprise-wide integration as directed by the Joint Chiefs of Staff, Assistant Secretary of Defense for Networks and Information Integration, and DoD Chief Information Officer.

The Contractor shall design and develop systems, sub-systems, and interfaces which conform to the latest approved Department of Health and Human Services Health Information Technology Standards Plan (HITSP) standards, as detailed in the OV-7a MHS Data Standards list.

The Contractor shall design and develop systems, sub-systems, and interfaces which conform to the DoD/MHS Health Data Definitions, DoD Global Information Grid architecture regarding the use of metadata and metadata registry products, MHS systems and interface architectural products, MHS Technical Standards Profile, Information Assurance Standards and Federal Health Technical Standards (which ever is most current). These products are available as GFI from the MHS Chief Architect via DHIMS architecture team.

The Contractor shall ensure that requirements and architectural products can be imported into MHS repositories (e.g. the Dynamic Object-Oriented Requirements System (DOORS), System Architect) and/or other databases in accordance with DoD NII EA tools.

The Contractor shall comply with Health Insurance Portability and Accountability Act (HIPAA) and the Defense Information Technology Standards Registry (DISR)/DHIMS TV-1, TV-2 and OV-7a when building or acquiring new software and/or software upgrades with Defense Health Program funds.

The Contractor shall provide a Work Breakdown Structure (WBS) that specifies tasks which include updates for the development, integration and review/approval and maintenance of architectural products at designated times during the life cycle of a given capability or system and how they intend to accomplish this work.

The Contractor shall provide architectural product status updates in the MPR.

Table 3-1
HITSP Approved Standards Documented in the Military Health System
Enterprise Architecture

<i>HL7 v 3.0 XML encoded</i>	<i>Adopt Health Level 7 messaging standards to ensure that each federal agency can share information that will improve coordinated care for patients such as entries of orders, scheduling appointments and tests and better coordination of the admittance, discharge and transfer of patients. Adopt Health Level & vocabulary standards for demographic information, units of measure, immunizations, and clinical encounter and HL7 Clinical Document Architecture standard for text base reports.</i>
<i>NCDCP SCRIPT</i>	<i>Adopt certain National Council for Prescription Drug Programs (Adopt certain National Council for Prescription Drug Programs (NCDCP) standards for ordering drugs from retail pharmacies to standardize information between health care providers and the pharmacies. These standards already have been adopted under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and today's announcement will make sure that parts of the three federal departments that aren't covered by HIPAA will also use the same standards.</i>
<i>ISO/IEEE11073</i>	<i>Adopt the Institute of Electrical and Electronics Engineers 11073 (ISO/IEEE 11073) series of standards that allow for health care providers to plug medical devices into information and computer systems that allow health care providers to monitor information from an ICU or through telehealth services on Indian reservations, and in other circumstances.</i>
<i>LOINC</i>	<i>Adopt laboratory Logical Observation Identifier Name Codes (LOINC) to standardize the electronic exchange of clinical laboratory results.</i>
<i>DICOM</i>	<i>Adopt Digital Imaging and Communications in Medicine (DICOM) standard that enable images, waveforms, and associated diagnostic information to be retrieved and transferred from various manufacturers' devices as well as medical staff workstations. Version 2006</i>
<i>SNOMED -CT</i>	<i>The College of American Pathologist's Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT) for laboratory result content, non-laboratory interventions and procedures, anatomy, diagnosis and problem lists, and nursing.</i>
<i>HIPAA</i>	<i>The Health Insurance Portability Accountability Act (HIPAA) transactions and code sets for electronic</i>

	<i>exchange of health related information to perform billing and administrative functions. These are the same standards now required under HIPAA for health plans, health clearinghouses and those health care providers who engage in certain electronic transactions.</i>
<i>Federal Terminologies</i>	<i>A set of federal terminologies related to medications, including the Food and Drug Administration's names and codes for ingredients, manufactured dosage forms, drug products and medication packages the National Library of Medicine's RxNORM for describing clinical drugs and the Veterans Administration's National Drug File Reference Terminology (NDF-RT) for specific drug classifications.</i>
<i>HUGN</i>	<i>The Human Gene Nomenclature (HUGN) for exchanging information regarding the role of genes in biomedical research in the federal sector.</i>
<i>EPA</i>	<i>The Environmental Protection Agency's Substance Registry System (SRS) provides a common basis/nomenclature for identification of non-medication chemicals, biological organisms and other substances. This recommendation is conditional based on addressing the healthcare requirements for access and use of the EPA system.</i>

The Contractor shall document if there are any DHIMS TV-1 or system architecture discrepancies, variances or exceptions to compliance with the MHS Enterprise Architecture. The Contractor shall submit metadata information for input into the MHS Metadata Registry. The Contractor shall develop and submit system architectural and interface products in accordance with IEEE and information assurance standards which include DHIMS mandated DoDAF architecture products*:

- All View architecture products (e.g., AV-1, AV-2);
 - Operational View architecture products (e.g., OV-1, OV-2, OV-3, OV-5, OV-6c, OV-7);
 - Systems and Services View architecture products (e.g., SV-1, SV-2, SV-4, SV-6, SV-10, SV-11);
 - Technical Standards View architecture products (e.g., TV-1, TV-2); and,
 - To include system and subsystem performance-based descriptions and key interfaces.
- Systems and Services Architecture views must clearly indicate requirements traceability to the Operational Architecture in the MHS EA.

*Sample list of architecture work products. Additional architecture artifacts may be required.

The Contractor shall update and maintain a Technical Standards Profile (TV-1) in coordination with the DHIMS architecture team.

The Contractor shall create a system that will follow guidance established in the DHIMS Development Guidance Packet (current version). The software should be written using Java technologies so it can be easily ported to a JSR 286 portlet in support of the future unified GUI. The software developed shall align with the future architecture as specified in the DHIMS Development Guidance Packet.

Internet Protocol version 6 (IPv6)

The Contractor shall provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are:

- Conformance to the DoD Information Technology Standards Repository (DISR) developed DoD IPv6 Standards Profile. Systems being developed, procured or acquired shall comply with the Global Information Grid Architecture and DISR standard IPv6 Capable definition. An IPv6 Capable system must meet the IPv6 base requirements defined in the “DoD IPv6 Standards Profile v1.0” dated June 1, 2006 available from the DISR.
- Maintenance of interoperability with IPv4. Systems being developed, procured or acquired shall maintain interoperability with IPv4 systems/capabilities. Systems should implement IPv4/IPv6 dual-stack and should also be built to determine which protocol layer to use depending on the destination host it is attempting to communicate with or establish a socket with. If either protocol is possible, systems should employ IPv6.
- Evidence of a migration path and commitment to upgrade all applications and product features to IPv6 by June 2008.
- Availability of Contractor/vendor IPv6 technical support for system development, implementation and management.

DoD IPv6 security guidelines, standards, and solutions shall be utilized and adhered to when available. Currently, DoD IPv6 Information Assurance (IA) guidance is available from the DoD IPv6 Transition Office (DITO).

6.4 Protection of Information

6.4.1 Dissemination of Information/Publishing

There shall be no dissemination or publication, except within and between the Contractor and any subContractors or specified Integrated Product/Process Team (IPT) members who have a need to know, of information developed under this order or contained in the reports to be furnished pursuant to this order without prior written approval of the TMA TM or the Contracting Officer. TMA approval for publication will require provisions which protect the intellectual property and patent rights of both TMA and the Contractor.

6.4.2 Contractor Employees

Contractor Identification

The Contractor shall ensure that Contractor personnel identify themselves as Contractors when attending meetings, answering Government telephones, providing any type of written correspondence, or working in situations where their actions could be construed as official Government acts.

Attendance at Meetings

Contractor personnel may be required to attend meetings or otherwise communicate with Government and/or other contract representatives to meet the requirements of this order. Contractor personnel shall make their Contractor status known during introductions.

Use of Military Rank by Contractor Personnel

Contractor personnel, while performing in a Contractor capacity, are prohibited from using their retired or reserve component military rank or title in all written or verbal communications associated with the contract under which they provide services.

6.4.3 Personally Identifiable Information (PII) and Protected Health Information (PHI)

The TMA Privacy Office website at <http://www.tricare.mil/tmaprivacy/contract.cfm> contains guidance regarding Protected Health Information (PHI) and Personally Identifiable Information (PII).

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data.

Health Insurance Portability and Accountability Act (HIPAA)

The Contractor shall comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191) requirements, as well as the Department of Defense (DoD) 6025.18-R, "DoD Health Information Privacy Regulation," January, 2003. This includes the Standards for Electronic Transactions, the Standards for Privacy of Individually Identifiable Health Information and the Security Standards. The Contractor shall also comply with all Applicable HIPAA-related rules and regulations as they are published and as Government requirements are defined (including identifiers for providers, employers, health plans, and individuals, and standards for claims attachment transactions). Any rules and regulations that are published and/or requirements that are defined after the award date of this contract, that require expenditure of additional Contractor resources for compliance may be considered "changes" and will be subject to the changes clause under the contract.

Systems of Record

In order to meet the requirements of 5 U.S.C. 552a, the Privacy Act of 1974, Contractors shall assist the TMA Privacy Office in completing a Privacy Act System of Records Notice for collections of records where information in identifiable form is retrieved. The Contractor will also comply with the requirements in Office of Management and Budget (OMB) Circular A-130, in the DoD Directive 5400.11, "DoD Privacy Program," May 8 2007, and in the DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007. The Contractor shall work with the Government point of contact to identify Privacy Act System of Records that are maintained or operated for TMA. Completed System of Records Notice formats for the applicable systems should be sent to the TRICARE Management Activity (TMA) Privacy Office at sormail@tma.osd.mil.

Privacy Impact Assessment

The Contractor shall provide for the completion of a Privacy Impact Assessment (PIA) for any applicable systems that collect, maintain, use or disseminate personally identifiable information (PII) or protected health information (PHI) about members of the public, Federal personnel, Contractors, or in some cases foreign nationals.

Contractors are responsible for the completion of the Privacy Impact Assessment Determination Checklist. This Checklist provides basic information to the TMA Privacy Office and ensures that the appropriate decision concerning PIA requirements is made. The Checklist can be downloaded from <http://www.tricare.mil/tmaprivacy/downloads/PIADC.121008.pdf>.

Contractors are responsible for the employment of practices that satisfy the requirements and regulations of the E-Government Act of 2002, (PubL. 107-347); DoD 5400.16-R, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009; Office of Management and Budget Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003, and current DoD PIA Guidance Memorandum at <http://www.tricare.mil/TMAPrivacy/Info-Papers-PIAs.cfm>. When completing a PIA, the Contractor is responsible for using the DoD-approved PIA Template, DoD Standard Form DD 2930, available at <http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2930.pdf>.

PIAs will be sent to the TRICARE Management Activity (TMA) Privacy Office at piamail@tma.osd.mil

Data Use Agreement (DUA)

A Data Use Agreement (DUA) is currently used to request Military Health System (MHS) data that is owned and/or managed by HA/TMA. The DUA ensures that applicable privacy and security requirements are followed in the use and/or disclosure of the data. To begin the DUA request process, contact duamail@tma.osd.mil. After receiving approval on a DUA, anyone needing access to information system applications or data sources managed by the Defense Health Services Systems (DHSS) will need to contact the DHSS Program Office at eidsaccess@tma.osd.mil to obtain information on access requirements. DUAs are active for one year, after which the Contractor must submit a renewal request or provide a Certificate of Data Destruction (CDD) to the TMA Privacy Office.

6.4.4 Business Associates

The TMA Privacy Office website at <http://www.tricare.mil/tmaprivacy/contract.cfm> contains standard contract clause language regarding Business Associates.

In accordance with DoD 6025.18-R "Department of Defense Health Information Privacy Regulation" the Contractor meets the definition of Business Associate. Therefore, a Business Associate Agreement is required to comply with both the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations. This clause serves as that agreement whereby the Contractor agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as defined in this clause, and DoD 6025.18-R and DoD 8580.02-R, as amended. Additional requirements will be addressed when implemented.

(a) *Definitions.* As used in this clause generally refer to the Code of Federal Regulations (CFR) definition unless a more specific provision exists in DoD 6025.18-R.

Individual has the same meaning as the term "individual" in 45 CFR 164.501 and 164.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

Protected Health Information has the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by the Contractor from or on behalf of The Government.

Electronic Protected Health Information has the same meaning as the term “electronic protected health information” in 45 CFR 160.103.

Required by Law has the same meaning as the term “required by law” in 45 CFR 164.501 and 164.103.

Secretary means the Secretary of the Department of Health and Human Services or his/her designee.

Security Rule means the Health Insurance Reform: Security Standards at 45 CFR part 160, 162 and part 164, subpart C.

Terms used, but not otherwise defined, in this Clause shall have the same meaning as those terms in 45 CFR 160.103, 164.501 and 164.304.

(b) The Contractor shall not use or further disclose PHI other than as permitted or required by the Contract or as Required by Law.

(c) The Contractor shall use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Award.

(d) The Contractor shall use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits in the execution of this Award.

(e) The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Health Information by the Contractor in violation of the requirements of this Clause. These mitigation actions will include as a minimum those listed in the TMA Breach Notification Standard Operating Procedure (SOP), which is available at: <http://www.tricare.mil/tmaprivacy/breach.cfm>

(f) The Contractor shall report to the Government any security incident involving protected health information of which it becomes aware.

(g) The Contractor shall report to the Government any use or disclosure of the PHI not provided for by this Award of which the Contractor becomes aware.

(h) The Contractor shall ensure that any agent, including a subContractor, to whom it provides PHI received from, or created or received by the Contractor on behalf of the Government agrees to the same restrictions and conditions that apply through this Contract to the Contractor with respect to such information.

(i) The Contractor shall ensure that any agent, including a subContractor, to whom it provides electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.

(j) The Contractor shall provide access, at the request of the Government, and in the time and manner designated by the Government to PHI in a Designated Record Set, to the Government. or, as directed by the Government, to an individual in order to meet the requirements under 45 CFR 164.524.

(k) The Contractor shall make any amendment(s) to PHI in a Designated Record Set that the Government directs or agrees to pursuant to 45 CFR 164.526 at the request of the Government or an Individual, and in the time and manner designated by the Government.

(l) The Contractor shall make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Contractor on behalf of, the Government, available to the Government, or at the request of the Government to the Secretary, in a time and manner designated by the Government or the Secretary, for purposes of the Secretary determining the Government's compliance with the Privacy Rule.

(m) The Contractor shall document such disclosures of PHI and information related to such disclosures as would be required for the Government to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

(n) The Contractor shall provide to the Government or an Individual, in time and manner designated by the Government, information collected in accordance with this Clause of the Contract, to permit the Government to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

General Use and Disclosure Provisions

Except as otherwise limited in this Clause, the Contractor may use or disclose PHI on behalf of, or to provide services to, the Government for treatment, payment, or healthcare operations purposes, in accordance with the specific use and disclosure provisions below, if such use or disclosure of PHI would not violate the Privacy Rule, the Security Rule, DoD 6025.18-R or DoD 8580.02-R if done by the Government.

Specific Use and Disclosure Provisions

(a) Except as otherwise limited in this Clause, the Contractor may use Protected Health Information for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

(b) Except as otherwise limited in this Clause, the Contractor may disclose Protected Health Information for the proper management and administration of the Contractor, provided that disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Clause, the Contractor may use PHI to provide Data Aggregation services to the Government as permitted by 45 CFR 164.504(e)(2)(i)(B).

(d) Contractor may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

Obligations of the Government

Provisions for the Government to Inform the Contractor of Privacy Practices and Restrictions

(a) Upon request the Government shall provide the Contractor with the notice of privacy practices that the Government produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) The Government shall provide the Contractor with any changes in, or revocation of, permission by Individual to use or disclose PHI, if such changes affect the Contractor's permitted or required uses and disclosures.

(c) The Government shall notify the Contractor of any restriction to the use or disclosure of PHI that the Government has agreed to in accordance with 45 CFR 164.522.

Permissible Requests by the Government

The Government shall not request the Contractor to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Contractor as otherwise permitted by this clause.

Termination

(a) Termination. A breach by the Contractor of this clause, may subject the Contractor to termination under any applicable default or termination provision of this Contract.

(b) Effect of Termination.

(1) If this contract has records management requirements, the records subject to the Clause should be handled in accordance with the records management requirements. If this contract does not have records management requirements, the records should be handled in accordance with paragraphs (2) and (3) below

(2) If this contract does not have records management requirements, except as provided in paragraph (3) of this section, upon termination of this Contract, for any reason, the Contractor shall return or destroy all Protected Health Information received from the Government, or created or received by the Contractor on behalf of the Government. This provision shall apply to Protected Health Information that is in the possession of subContractors or agents of the Contractor. The Contractor shall retain no copies of the PHI.

(3) If this contract does not have records management provisions and the Contractor determines that returning or destroying the Protected Health Information is infeasible, the Contractor shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the Contractor that return or destruction of PHI is infeasible, the Contractor shall extend the protections of this Contract to such PHI and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as the Contractor maintains such PHI.

Miscellaneous

(a) Regulatory References. A reference in this Clause to a section in DoD 6025.18-R, DoD 8580.02-R, Privacy Rule or Security Rule means the section as in effect or as amended, and for which compliance is required.

(b) Survival. The respective rights and obligations of Business Associate under the "Effect of Termination" provision of this Clause shall survive the termination of this Contract.

(c) Interpretation. Any ambiguity in this Clause shall be resolved in favor of a meaning that permits the Government to comply with DoD 6025.18-R, DoD 8580.02-R, Privacy Rule or Security Rule

6.4.5 Public Key Infrastructure Authentication and Encryption.

Contractors shall follow the DoD standards, policies, and procedures related to the use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication including authentication to DoD private web servers or applications. Where interoperable PKI is required for the exchange of unclassified information, including the encryption of e-mail containing sensitive information, between DoD and its vendors and Contractors, industry partners shall obtain all necessary certificates if they are not eligible for a DoD Common Access Card. (refer to <http://iase.disa.mil/pki/eca/> and <http://www.cac.mil/>).

6.5 Access Requirements

6.5.1 Contractor access to HA/TMA Network/DoD Systems

The TMA Privacy Office website at <http://www.tricare.mil/tmaprivacy/contract.cfm> contains guidance regarding Contractor access to the HA/TMA Network/DoD Systems.

The Contractor shall contact the COR after being awarded a contract if access to a DoD system is required. The Contractor is responsible for submitting the SF85P and FD 258 for their respective Contractor employees if the Contractor employees are required to gain access to a DoD system for performance of this contract. As such, Contractor personnel shall undergo appropriate background investigation (Trustworthiness Determination for Public Trust positions/ADP-IT) or have a security clearance and Information Assurance training if deemed necessary. The Contractor should be prepared for this process to take at least two (2) weeks.

Prior to the submission of the SF85P for new Contractor employees, the Contractor's Facility Security Officer (FSO) shall submit the contract number, contract start date, contract end date, personnel names, and the ADP position designations, to the designated CORs for verification and approval with a list of personnel being submitted for an ADP/IT Trustworthiness Determination. The Contractor's FSO shall submit all appropriate forms as provided by the CORs to request a background investigation to the Office of Personnel Management (OPM) and obtain receipt confirmation as a prerequisite for Contractor personnel to access DoD systems. The Standard Form 85P is available at: <http://www.tricare.osd.mil/tmaprivacy/sf85p.pdf>.

The Contracting company shall ensure all Contractor personnel are designated as ADP/IT-I, ADP/IT-II where their duties meet the criteria of the position sensitivity designations.

The Contractor must notify the COR when the security officer has submitted the SF85P user form to OPM for new employees. Upon termination of a Contractor employee from the contract, the Contractor's FSO must notify the COR and OPM of the action, including the termination date. In both cases, the COR must notify the Deputy Director, TMA Privacy Office at Pamela.Schmidt@tma.osd.mil. All emails should be sent using CAC encryption.

The TMA Privacy Office website at <http://www.tricare.mil/tmaprivacy/contract.cfm> contains guidance regarding Contractor access to the HA/TMA Network/DoD Systems.

Contracting companies shall contact the TMA Privacy Office after being awarded a TRICARE contract that requires access to a DoD system. Each contracting company is responsible for

submitting the SF85P and FD 258 for their respective Contractor employees. The Contractor employees may be required to gain access to the HA/TMA network/Program Office system for performance of this task. As such, Contractor personnel shall undergo appropriate background investigation (Trustworthiness Determination for Public Trust positions/ADP-IT) or have a security clearance and Information Assurance training. The Contractor should be prepared for this process to take at least two (2) weeks.

Prior to the submission of the SF85P for new Contractor employees, the Contractor's Facility Security Officer (FSO) shall submit the TRICARE contract number, delivery order number, contract start date, contract end date, personnel names, and the ADP position designations, to the TMA Privacy Office for verification and approval with a list of personnel being submitted for an ADP/IT Trustworthiness Determination. The Contractor's FSO shall submit all appropriate forms as listed on the TMA Privacy website to request a background investigation to the Office of Personnel Management (OPM) and obtain receipt confirmation as a prerequisite for Contractor personnel to access the HA/TMA network/TRICARE Program Office systems. The Standard Form 85P is available at: <http://www.tricare.osd.mil/tmaprivacy/sf85p.pdf>.

The Contracting company shall follow the TMA Privacy Office guidelines for submittal of ADP/IT security clearances and ensure all Contractor personnel are designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III where their duties meet the criteria of the position sensitivity designations. The TMA Privacy Office procedures for personnel security are listed on the following website: <http://www.tricare.osd.mil/tmaprivacy/personnel-security.cfm>.

Contracting companies must notify the TMA Privacy Office when the security officer has submitted the SF85P user form to OPM for new employees. Upon termination of a Contractor employee from the TRICARE Contract, the Contractor's FSO must notify the TMA Privacy Office and OPM of the action, including the termination date. At the end of the base period of performance, the contracting companies shall notify the TMA Privacy Office if the contract has been extended for the option years or terminated.

Non-U.S. Citizens

Only U.S. citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless approved. Exceptions to these requirements shall be permitted only for compelling national security reasons. (DoD 5200.2-R, C2.1.1, AP6.6.1) Non-U.S. citizens are not being adjudicated by any government agency for a trustworthiness determination at this time. Non-U.S. Citizens are not allowed access to any DoD systems/networks

Deleted: by an authority designated in Appendix 6 etc

The Contractor shall ensure that data which contains PHI is continuously protected from unauthorized access, use, modification, or disclosure. The Contractor shall comply with all previously-stated requirements for HIPAA, Personnel Security, Electronic Security, and Physical Security.

Termination of access

Upon termination of a Contractor employee the Contractor Point of Contact shall forward a request to have the employee deleted from DoD system access to the COR.

6.5.2 Contractor Access to Classified Information

The Contractor will require access to classified data to perform this task.

6.6 Development

All telecommunications network designs shall make maximum use of existing telecommunications infrastructure. All MHS system modifications and new development shall comply with the latest version of the DoD Joint Technical Architecture and any other applicable DoD and MHS technical standards and policies. The goal of the MHS architectural framework is to use the Defense Information Infrastructure Common Operating Environment (DII COE) to support the MHS, as required. The MHS will emphasize both software reuse and interoperability and incorporate the DII COE standards as applicable. All new systems development and new development in deployed migration systems will use DoD data standards in accordance with PDASD – HA policy memo, “Use of DoD Standards in MHS Migration Systems,” of 11 March 1996.

6.7 Data Rights

All software and related data rights developed or provided under this order, including any commercial off the shelf or previously proprietary software, will be provided to the Government, for any intended use by the Government, consistent with, and in compliance with DFARS: (applicable as though fully set forth)

- 252.227-7013 Rights in Technical Data-Noncommercial Items
- 252.227-7014 Rights in Noncommercial Computer Software & Documentation
- 252.227-7015 Technical Data – Commercial Items
- 252.227-7016 Rights in Bid or Proposal Information
- 252.227-7017 Identification and Assertion of Use or Restrictions
- 252.227-7019 Validation of Asserted Restrictions
- 252.227-7020 Rights in Special Works
- 252.227-7022 Government Rights (unlimited)
- 252.227-7023 Drawings and Data to become Property of Government
- 252.227-7025 Limitations on the Use or Disclosure of GFI
- 252.227-7027 Deferred Ordering of Technical Data or Software
- 252.227-7028 Technical Data or Software Previously Delivered
- 252.227-7030 Technical Data - Withholding of Payment
- 252.227-7037 Validation of Restrictive Markings on Technical Data

6.8 Quality Assurance

The Government will review monthly performance and progress reports and will attend regular task performance review meetings with the Contractor to survey quality of products and services.

6.8.1 Quality Assurance Surveillance Plan (QASP)

The Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor’s performance. The oversight provided for in the order and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the required Past Performance Information Assessments. The QASP will be finalized immediately following award and a copy provided to the Contractor after award. The QASP is a living document and may be updated by the Government as necessary.

6.8.2 Performance Requirements Summary Matrix

By monitoring the Contractor, the COR will determine whether the performance levels set forth in the order have been attained. Incentives for meeting or not meeting the performance standards shall be reflected in a positive past performance rating and the award of subsequent option years.

Desired Outputs	Required Service	Performance indicators	Monitoring Method
Development objectives – completion of development activities as stated in the above objectives including but not limited to: stabilize the features in AHLTA and CHCS., enhance the functionality of the Theater suite, GUI development to provide access to the current EHR capabilities.	All functional requirements shall be met; software delivered shall comply VA and DOD standards and enterprise architecture technologies when practical.	OCD results will be analyzed in accordance with the Quality Assurance Plan (QAP) as developed by the Contractor and TMA program office.	Analyses of OCD and user feedback. Review associated documentation
Software rollout and integration - Interfaces with all system components are fully functional and seamlessly integrated.	Software shall pull Data from VA and DOD enterprise systems, such as AHLTA, CHCS, VistA	End user satisfaction and software performance.	End user feedback. Review of site and user surveys
Software usability - Software capable of performing the requisite functions shall be delivered in accordance with the stated objectives	Delivery dates set forth are met or exceeded. Development Release implemented.	Delivery dates shall be met unless government and Contractor agree to a new submission date.	End user feedback and Program management observation

6.8.3 Performance Evaluation Process

The Contractor Performance Assessment Reporting System (CPARS) has been adopted by TMA to electronically capture assessment data and manage the evaluation process. CPARS is used to assess a Contractor's performance and provide a record, both positive and negative, on a given contract during a specific period of time. The CPARS process is designed with a series of checks and balances to facilitate the objective and consistent evaluation of Contractor performance. Both government and Contractor program management perspectives are captured on the CPAR form and together make a complete CPAR. Once the Assessing Official completes the proposed assessment for the period of performance, the CPARS is released to the appropriate Government Contractor Representative for their review and comments. User ID and Password will be provided to the designated Government Contractor Representative upon issuance of a task order. The Contractor has 30 days after the Government's evaluation is completed to comment on the evaluation. The Government Contractor Representative must either concur or nonconcur to each CPAR. If the Contractor concurs with the proposed assessment and the Reviewing Official does not wish to see the CPAR, the Assessing Official may close out the CPAR. Otherwise, they must

forward the CPAR to the Reviewing Official for them to review, enter comments if appropriate, and close out. The Reviewing Official may at their option direct the Assessing Official to forward every CPAR to them for review.

6.9 Government Furnished Equipment (GFE)/ Information (GFI)/Facilities

Any hardware additions/updates for production use (configuration & costs) above the current infrastructure to support these fixes will be provided as Government Furnished Equipment (GFE).

6.9.1 Government Facilities

Not applicable.

6.9.2 Government Furnished Equipment/Information/Property

The Contractor shall maintain a detailed inventory accounting system for Government Furnished Equipment/Material or Contractor-Acquired-Government Owned Property (CAP). The inventory accounting system must specify, as a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if CAP), and contract/order number under which the equipment is being used. The Contractor shall either: a) attach an update inventory report to each monthly performance and progress report, or b) certify that the inventory has been updated and is available for Government review. In either case the Contractor's inventory listing must be available for Government review within one business day of COR request.

6.10 Section 508 Requirement

The Contractor shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d). Specifically, the procurement, development, maintenance, or integration of electronic and information technology (EIT) under this contract must comply with the applicable accessibility standards issued by the Architectural and Transportation Barriers Compliance Board at [CFR part 1194](#).

6.11 Earned Value Management (EVM) Reporting

The Contractor shall use an Earned Value Management System (EVMS) in compliance with DFARS clauses 252.234-7001 and 252.234-7002 to plan, track, and manage program activities. The Contractor shall provide Contract Performance Reports (CPRs) in accordance with the requirements of DID DI-MGMT-81466A, "Contract Performance Report (CPR)." For awards valued over \$50 million, all CPR formats must be reported. For awards valued at or over \$20 million, but under \$50 million, the CPR may be tailored to CPR Format 1 (Work Breakdown Structure), Format 3 (Baseline), and Format 5 (Explanations and Problem Analyses) if requested by the Contractor and approved by the COR. For awards valued under \$20 million, but containing an EVM requirement, the CPR may be tailored to CPR Format 1 (Work Breakdown Structure), and Format 5 (Explanations and Problem Analyses) if requested by the Contractor and approved by the COR. The Contractor shall prepare Contract Funds Status Reports (CFSR) in accordance with DID DI-MGMT-81468, "Contract Funds Status Report." The level of detail to be provided in the CFSR will be coordinated with and approved by the TMA COR.

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Font: Not Bold

7.0 APPLICABLE DOCUMENTS AND DEFINITIONS

7.1 Compliance Documents and Reference Documents

The Contractor shall adhere, to the extent applicable to the Contractor's obligations, to the policy and procedures as outlined in the documentation indicated below. The Contractor shall also adhere to any laws, regulations, policies, procedures, and guidelines relevant to the specific tasks being performed in this DO.

- Defense Data Dictionary System (DDDS), 29 May 2002
- EIA-649A, "National Consensus Standard for Configuration Management"
- Health Insurance Portability and Accountability Act of 1996
- Health Insurance Portability and Accountability Act of 1996 (Privacy Rule) effective October 15, 2002
- Health Insurance Portability and Accountability Act of 1996 (Security Rule) effective April 21, 2003
- Privacy Act of 1974, (5 U.S.C. 552a eq. seq)
- DoD 5000 Series, current version, (<http://akss.dau.mil>)
- MHS Information Assurance (IA) Policy/Guidance Manual, Version 1.3, February 2003 (www.tricare.osd.mil/tmis_new/ia.htm#mhs)
- DoD 5200.2-R, "Personnel Security Program," current version(<http://www.dtic.mil/whs/directives/corres/html/520002r.htm>)
- DOD 5200.1-R Information Security Program, current version, (<http://www.dtic.mil/whs/directives/corres/html/520001r.htm>)
- DoD Information Technology Standards Registry (DISR), current version, (<https://disronline.disa.mil/>)
- MHS Enterprise Architecture (Updated online and available at (www.tricare.osd.mil/Architecture))
- DoD 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, current version(<http://www.dtic.mil/whs/directives/corres/html/851001m.htm>)
- Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 4.0, dated 4 October 99, and subsequent updates
- DoD 5400.11-R, DoD Privacy Program, current version, (<http://www.dtic.mil/whs/directives/corres/html/540011r.htm>)
- DoD Directive 8500.1, "Information Assurance (IA)," current version(<http://www.dtic.mil/whs/directives/corres/html/850001.htm>)
- DoD Instruction 8500.2, "Information Assurance (IA) Implementation," current version(<http://www.dtic.mil/whs/directives/corres/html/850002.htm>)
- DoD 6025.18-R, "DoD Health Information Privacy Regulation", dated current version, (<http://www.dtic.mil/whs/directives/corres/html/602518r.htm>)
- DoD Instruction 8551.1, "Ports, Protocols, and Services Management," current version, (<http://www.dtic.mil/whs/directives/corres/html/855101.htm>)
- Clinger-Cohen Act of 1996, 40 U.S.C. 1401 et seq.
- DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," current version, (<http://www.dtic.mil/whs/directives/corres/html/858001.htm>)
- DOD Architecture Framework Version 1.0, February 9, 2004 (<http://www.defenselink.mil/cio-nii/cio/earch.shtml>)

- CJCSI 3170.01E Joint Capabilities Integration and Development System, May 11, 2005 (http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm)

Approval

For Administrative Purposes Only

COL Claude Hines, Jr., USA, MS
Program Manager
Defense Health Information Management System

Date

APPENDIX A- EHR System Defects and SCRs



APPENDIX A - EHR
System Defects and SCRs

APPENDIX B – AHLTA 4.0 Prototype Capability Matrix



APPENDIX B – AHLTA
4.0 Capability Matrix.

APPENDIX C-AHLTA 4.0 Prototype Baseline Functionality



APPENDIX C-AHLTA
4.0 Baseline Function

APPENDIX D- MHS Information Assurance Requirements



APPENDIX D- MHS
Information Assurance

APPENDIX E- Enterprise Architecture Standards



APPENDIX E -
Enterprise Architecture

APPENDIX F- FHCC Functional Requirement



APPENDIX F - FHCC
Functional Requirements

APPENDIX G- Current Functionality



APPENDIX G-
Current Functionality

APPENDIX H - Problem Description for the EHR Architecture



APPENDIX H - EHR
Architecture Problem

APPENDIX I - Proprietary COTS Software and Dependencies



APPENDIX I -
Proprietary COTS Sof

APPENDIX J- Architecture Diagrams

Documents available pre- award in the technical library.

Deleted: attached separately

APPENDIX K – DHIMS Web Service Mapping



APPENDIX K - DHIMS
Web Service Mapping

APPENDIX L – Technical Specifications for Patient Registration Service



Appendix L -
Technical Specification

APPENDIX M - Government Furnished Information

Certain aspects of this current list of capabilities can be furnished as GFI for the purposes of potential rewrite, COTS replacement, or integration to meet the intent of the objectives listed above. Justification for which components, why and projected outcome of these components as part of the objectives listed above is expected as part of the proposal. There may be limitation to the degree (e.g. source code) of GFI availability on any COTS products like Essentris or 3M Care Innovation Suite.

Completed products

These capabilities are completed products that may be considered as potential GFI to include source code with the exception of 3rd party products (widgets) that are COTS components.

AHLTA 3.3 is the current enterprise-wide medical and dental clinical information system that provides secure online access to longitudinal health records. AHLTA enables MHS providers to document a patient's health information and history, which are consolidated in a single clinical database known as the Clinical Data Repository (CDR) and are made accessible to authorized users worldwide, 24 hours a day. The CDR facilitates trend analysis activities and medical surveillance at the patient or population level. Providers can access executive-level reports on common diagnoses and procedures to identify trends of concern. AHLTA also incorporates all Computer-based Provider Order Entry (CPOE) capabilities with a user-friendly interface to improve coding practices and expand the documentation of medical care. Additionally, Healthcare Artifact and Image Management Solution (HAIMS) will provide an Enterprise Content Management capability for managing non-computable parts of the medical record, such as EKGs, consent forms and discharge summaries. AHLTA 3.3 has been pre-certified by the Certification Commission for Healthcare Information Technology (CCHIT). AHLTA 3.3 which is currently in deployment builds upon the AHLTA baseline and provides a number of functional enhancements to include but not limited to:

- Encounter Documentation and Coding
- Problem List Generation

- Order Entry
- Results Retrieval
- Consult Tracking
- Allergies Warning
- Medical Alerts
- Immunization Documentation
- Wellness Reminders
- Self-Reporting Tools

AHLTA 4.0 converges the functional base lines of both AHLTA 3.3 and AHLTA theater into one common functional baseline to deliver a more seamless “train as you fight” experience within the system. The single baseline will have the same code base, and have the same look, feel and functionality while improving the capability of the Theater system by bringing its baseline up to that of Sustaining Base, allowing the warfighters to train as they fight. The Theater portion of the application is currently in DT&E. The Garrison portion of the application has not been tested and has known issues. The efforts to stabilize AHLTA 3.3 may potentially result in a divergent baseline where fixes identified and addressed in AHLTA 3.3 have not been addressed in AHLTA 4.0. Capabilities include but are not limited to:

- Electronic Patient Signature
- Emergency Room (ER) Front End
- Electronic Standard Forms (ESF) Tool
- Integrated Immunizations (Main Module)
- Improved Readiness
- Improved Screening Module
- Personnel Reliability Program (PRP)
- Injury Cause Coding (ICC)
- Improved Medical Profiles
- HART-A (Health Assessment Review Tool “Accession” variant “HART-A”)
- Navy Individual Medical Readiness (IMR)

Deployed Tele-Radiology System (DTRS) is currently deployed and serves as the Picture Archiving and Communications System (PACS) for Theater. Manages images generated from Digital X-Ray (DX), Computed Radiography (CR) and CTs in Theater. System allows the transfer of radiographic images via the theater communications infrastructure intra-theater and on to Landstuhl Provides onsite personnel for technical support in Iraq, Afghanistan and Kuwait

Legacy Composite Health Care System (CHCS) is in production and enables DoD providers to electronically perform patient appointment processes and scheduling, order laboratory tests, retrieve test results, authorize radiology procedures and prescribe medications within AHLTA. CHCS continues to be one of the most broadly used CPOE systems in the nation, and it also supports multiple healthcare administration activities, including patient administration, medical service accounting, medical billing and workload assignments. This backbone is currently built upon legacy technology that is currently being restructured to deliver the capabilities outlined below in a modular, reusable method that is standards based and in accordance with best industry practices.

CHCS modules provide automated features and capabilities in support of the following:

- Patient Administration
- Patient Appointments and Scheduling

- Managed Care Program
- Quality Assurance
- Dietetics
- Laboratory
- Radiology
- Pharmacy
- Workload Accounting Module
- Medical Services Accounting
- Ambulatory Data Module
- Medical Records Tracking
- Database Administration
- Order Entry/Results Retrieval

CHCS interfaces with 60 other clinical and administrative systems, including:

- VA Consolidated Mail Outpatient Pharmacy (VA CMOP)
- TRICARE Online (TOL)
- Pharmacy Data Transaction Service (PDTS)
- Defense Medical Logistics Standard Support (DMLSS)
- Third-Party Outpatient Collection System (TPOCS)
- Defense Blood Standard System (DBSS)
- Defense Enrollment Eligibility Reporting System (DEERS)
- HART 2B

CHCS provides enhanced health assessment and readiness questionnaires, expands the data shared with the Clinical Data Mart (CDM) for reporting and nearly doubles the speed of data shared with the CDM. The questionnaires provide service members the capability to document personal health information that will then be reviewed by a provider in the EHR. The data collected over time will provide a more complete clinical picture of the readiness and health status of the beneficiary during the service member's life cycle with the military. This capability is currently in testing and expected to begin deployment following EHR stabilization.

Federal Health Information Exchange (FHIE) enables the transfer of electronic health information to the VA at the time of a Service member's separation. DoD transmits data to VA on a monthly basis: inpatient and outpatient laboratory and radiology results, outpatient pharmacy data, allergy information, discharge summaries, consult reports and demographic data. VA providers and benefits specialists access this data daily for use in the delivery of healthcare and claims adjudication.

Bidirectional Health Information Exchange (BHIE) allows DoD and VA providers to view clinical information in real-time for patients who receive care in either agency health system. BHIE enables the bidirectional sharing of allergy information; outpatient pharmacy data; demographic data; inpatient and outpatient laboratory and radiology results; Theater clinical data; and vital signs. Access to BHIE data is available through AHLTA, the military's EHR, and through VistA, VA's EHR, for patients treated by both departments.

Pre- and Post-Deployment Health Assessment Forms Sharing (PPDHA) DoD sends electronic (PPDHA) and Post-Deployment Health Reassessment (PDHRA) data to the VA monthly for separated Service members, National Guard, and Reserve members who have been

deployed and are now demobilized. In addition, DoD sends VA weekly data pulls of PDHRAs for individuals referred to the VA for care or evaluation.

Clinical Data Repository/Health Data Repository (CHDR) establishes interoperability between DoD's Clinical Data Repository and VA's Health Data Repository by incorporating the exchange of standardized data into each agency's EHR. This integrates outpatient pharmacy and medication allergy data for shared patients. Exchanging standardized pharmacy and allergy data supports the ability to conduct drug-drug and drug-allergy interaction checking using data from both DoD and VA.

Laboratory Data Sharing Initiative (LDSI) facilitates the electronic sharing of laboratory orders and results between DoD, VA, and/or commercial reference laboratories. LDSI is actively being used on a daily basis between DoD and VA at several sites where one facility uses the other as a reference lab. Either Department may function as the reference lab for the other with electronic order entry and results retrieval. Additionally, LDSI enhances patient safety by eliminating potential clerical errors resulting from manual transcription of orders and results from paper into the computer system.

AHLTA-Mobile is the first responder's handheld data capture device. AHLTA-Mobile allows for immediate documentation of injury, illness and care, and stores medical data until it is transferred to AHLTA-Theater. AHLTA-Mobile can electronically store medical reference documents and replaces pounds of books and paper previously carried by medics. AHLTA-mobile is currently being enhanced to support finger-friendly (non-stylus based) user input to the EHR on a Personal Digital Assistant (PDA). The process of capturing and documenting data will be simplified, faster, and more intuitive to the user.

AHLTA-Theater extends the sustaining-base electronic medical record (AHLTA) capability, look and feel to the Theater of operation. AHLTA-Theater enables healthcare providers to document care, order laboratory services such as blood work, x-rays and medications, and store medical data until communications are available to send the data to the Theater Medical Data Store and Clinical Data Repository.

TMIP Composite Health Care System Caché (TC2) provides documentation for inpatient healthcare, ancillary services order-entry, and result-reporting in the deployed environment. TC2 provides inpatient management, laboratory, radiology, and pharmacy ordering capabilities, and enables users to schedule outpatient clinic and radiology procedures. This capability is currently being restructured in concert with the Legacy CHCS effort to provide a modernized interface to improve usability of the system with a friendlier graphical user interface along with the efforts to improve the performance of the system architecturally.

SNAP Automated Medical System (SAMS) is a Navy-specific shipboard legacy healthcare information system phasing out as similar TMIP capabilities emerge. Key capabilities include: electronically documents care; documents and records environmental and occupational exposures; manages medical materiel; and records and tracks medical readiness. The capabilities of SAMS are being integrated into the enterprise systems to deliver this Service specific need. Upon capability integration, this service specific system will be retired.

Theater Medical Data Store (TMDS) captures information from the Theater medical systems and serves as the authoritative Theater database for collecting, distributing and viewing Service members' pertinent medical information. TMDS updates the AHLTA CDR, where all Service members' EHRs reside. This information is also made available to the VA through the

bidirectional interface, BHIE. TMDS integrates the Joint Patient Tracking Application functionality to view, track and manage ill or injured patients as they move through the theater levels of care, sustaining-base Military Treatment Facilities and those facilities shared with the VA. Enhancements to this application have been made to provide the initial capability to document and track mild traumatic brain injury and secure behavioral health encounters. A number of user interface enhancements are made to improve the user workflow to better support the medical business practice. There is also a project currently under way to allow for continuity of operations at an alternate computing facility in the event of primary facility disruption.

Joint Medical Workstation (JMeWS) provides medical situational awareness, medical surveillance, and force health decision support. It also reports on medical trends and analyzes the overall status of theater health. JMeWS provides the ability to drill down to specific medical units and individual encounters. It also shares medical intelligence with GCSS and GCCS, serving as the medical component to the Combatant and Joint Task Force Commander's common operating picture. Enhancements to this application are being made to help track blood products logistically. There is also a project currently under way to allow for continuity of operations at an alternate computing facility in the event of primary facility disruption.

Joint Medical Analysis Tool (JMAT) is a Joint Staff approved automated application that provides joint medical planners and decision-makers a tool to support, deliberate, and crisis action planning. The tool assists the calculation and generation of theater medical requirements, scenario development to support course-of-action analysis, and risk assessment to plan the allocation of critical medical resources. This system is being modernized to better meet the customer's needs in a framework that is more standards based for better integration into the Command and Control systems.

Patient Movement Items Tracking System (PMITS) PlexusD is currently under sustainment and tracks the storage of PMI during peacetime and its movement during contingency and wartime operations. PMITS PlexusD directly supports the Warfighters' mission by ensuring critical patient movement equipment is available to save critically injured Warfighters' lives. Commanders use PMITS PlexusD to manage and redistribute PMI assets to avoid shortages during patient evacuations.

TMIP Framework provides a messaging service to DHIMS applications allowing electronic health records and other medical information to be transmitted from the theater to CONUS repositories, such as JMeWS and TMDS. The TMIP Framework is designed to work in environments with low or interrupted communications, thereby guaranteeing critical medical data is available to healthcare providers and decision makers. This framework is currently being enhanced to improve reliability of message transport, improved scalability to handle greater volumes of information while reducing administration of this capability.

Coordination Activities

These products and services are currently in development and will require coordination activities which may include some GFI but may not fully functional. They should not be considered complete or a dependency to accomplishing the tasks within the SOO due to the in-progress state of these activities.

Neuro-Cognitive Assessment Tool is currently under limited user testing to enable baseline and post-event screening of possible mild traumatic brain injuries (mTBI) across all services at all echelons of care, including all levels of Theater and the sustaining base. NCAT was selected by

DoD to provide a capability for early assessment, supporting diagnosis, and monitoring patients with possible mTBI

- Captures baseline neurocognitive assessments on Armed Forces personnel
- Compare results across current, baseline and normative population
- Use in Theater and Sustaining base at all levels of care
- Track and trend TBI data in a centralized database
- Provide de-identified information for research
- Can be administered by a non-medical personnel
- Provide neurocognitive testing data that may aid in the detection/diagnosis of mTBI

Health Artifact and Imaging Solution (HAIMS) is beginning limited user testing to provide a web-enabled capability for DoD and the VA healthcare providers to have global access and global awareness of documents and images generated during the healthcare delivery process. This solution will be delivered in a three Phased Approach. Phase I provides a Web based standalone for DOD, access by VA through BHIE (current PoP) Import, View, Edit, Register, Manage, and Store various types of documents and images Pictures, Scanned documents, video files, audio files, PDF files, CDA R2, XML, MS Office

HAIMS Phase II will expand on the capabilities described in Phase I and:

- Expand the development effort to associate documents and images with patient encounters.
- Provide users an extension to the EHR user interface so that the presence of A&I will be made apparent in the proper clinical context, including associated encounters, radiology and other specialty reports, and dental documentation.
- Provide users rapid access to high interest A&I, such as the most recent available EKG or set of dental bite wing radiographs, enhancing productivity by reducing the number of steps a provider must take to find A&I.
- Allow clinical users to upload (“publish”) A&I to a HAIMS repository within the workflow of documenting clinical notes in AHLTA. Not having to navigate to a separate application will enhance the user experience and productivity and will enable the A&I to be attached to the correct event.

Clinical Case Management (CCM), Disability Evaluation System (DES) and Pay Interface currently under development supports the mission of transitioning disabled Service Members toward their separation or retirement while providing enterprise capability to allow for collection and tracking of sentinel Medical Evaluation Board and Physical Evaluation Board events. It also allows access to records and information deemed necessary to support the Disability Evaluation process from clinical and business areas. DES supports business process re-engineering efforts between VA and DoD to provide a faster and more consistent evaluation and transition for wounded Service Members. It enables the collection, reporting, and enterprise visualization of CCM information that is not available within the current AHLTA system. This project also provides necessary Admission-Discharge-Transfer (ADT) messaging to the pay systems, allowing for proper processing of changes in patient payroll status and financial entitlements.

AHLTA Enhancements is currently under development to provide a common IBM Workplace forms web-enabled service. This service will allow integration into other applications and messaging in various formats to various destinations.

Integrated Clinical Data Base (ICDB) The Integrated Clinical Data Base is an Air Force, portal-like, clinical web application. ICDB consolidates data from multiple clinical sources,

mainly CHCS and SARD, into an Oracle database for presentation to the provider. In addition to a GUI based presentation of CHCS data, ICDB allows for some data entry, which is confined to ICDB, but available for viewing throughout the MTF, as well as any other MTF that shares the same CHCS host. Each ICDB instance is paired with a single CHCS host. The government will help coordinate this product as a potential GFI with the Air Force.

AHLTA Stabilization- is currently under development to provide initial AHLTA application and central data repository (CDR) stabilization efforts will improve the reliability of AHLTA and the CDR by providing a hot failover. This effort will optimize some of the middle ware products. This effort implement a process to periodically reclaim CDR space and to reduce CDR database growth by removing unused and less frequently used data in CDR. Reducing the CDR database size will result in improved backup and recovery process, thereby improving CDR's availability and reliability. This effort will also prepare the CDR for replication technologies in the future to regionalize the information for better performance and continuity of operation.

Universal Immunization is currently in development by the Air force and provides a single web-based interface for all clinical and reporting systems based on AFCITA that are involved in the immunization workflow. This effort will bring the immunization master record within the MHS enclave. This also supports the immunization community's needs to readily update immunizations, routes, methods, inventories and reporting needs across the DoD.

Enterprise Blood Management is currently in the acquisition process which will provide an enterprise-wide blood information capture, tracking, and management system. This will improve the current MHS blood capabilities to support both the sustaining base and theater specific needs. It will also support improved logistical planning for the blood supply and improves the ability for post-incident tracking in events where blood is needed before it can be tested. This system closes the capability gap by making blood management data accessible worldwide.

Bidirectional Health Information Exchange (BHIE 5) is currently under development which will improve the performance of the DoD/VA data sharing framework by making data available faster and expanding the data sharing set to include NCAT information in a manner viewable to the VA. Additionally, it will allow DoD and VA providers to view clinical information in real-time for patients who receive care in either agency health system. Ultimately, BHIE will enable the bidirectional sharing of allergy information; outpatient pharmacy data; demographic data; inpatient and outpatient laboratory and radiology results; theater clinical data; and vital signs. Access to BHIE data is available through AHLTA, the DoD's EHR, and through VistA, VA's EHR, for patients treated by both departments.

DOD Occupational and Environmental Health Readiness System - Industrial Hygiene (DOEHRS-IH) is currently in development which will support the reduction of worksite hazards and supports the tracking of long-term environmental exposure. DOEHRS-IH provides analytical support for documenting occupational hazards by capturing analysis results of air, water and soil samples. This capability currently under development will permit the retirement of the legacy Service-specific environmental and industrial health applications (SAMS Environmental Health [EH] and GEMS Theater Occupational Module [TOM] & Public Health Deployed [PHD]). Additionally, it simplifies architecture by retiring legacy components.

U.S. Transportation Command Regulating and Command & Control Aero-medical Evacuation System (TRAC2ES) Interface with TMDS is currently under sustainment to monitor and track patients leaving theater via Air Force aero-medical evacuation. The system provides visibility of the logistics of incoming and outgoing flights and enables scheduling of

patients' departures. TRAC2ES interfaces with TMDS, receiving pertinent health care information from the electronic medical record and sending information to enable patient movement visibility.

Medical Situational Awareness in the Theater (MSAT) is currently in development which is an Advanced Concept Technology Demonstration currently in development that combines information from multiple communities to provide a common operating picture and decision support for the Combatant and Joint Task for Commanders Surgeon staffs. MSAT leverages Service Oriented Architecture combining medical, patient tracking, mapping, logistics, personnel, weather, and intelligence information to support current and planned operations decision making. The MSAT standards based information sharing approach enables rapid connection to current and emerging information sets reducing integration costs while adding increased value over time.

Virtualization is currently in the acquisition process which will provide application streaming for specific parts of a computer program to be available at any instance for the end user to perform a particular function. This means that a program need not be fully installed on a client computer, but parts of it can be delivered over a low bandwidth network as and when required. Furthermore, it will be able to deliver client based products over the web as part of the GUI framework. This virtualizes server components to maximize computing resources and reduce sustainment. Additionally, it virtualizes the storage to pool various physical devices into a logical array that allows storage to be in a number of locations physically, but appear to be a single source.

Regionalized Data Centers is currently in the acquisition process which will result in improved performance of information retrieval and improved reliability of documenting and gathering that information consistent with industry best practices. This major infrastructure enhancement will build a redundant and performance oriented data framework that will be leveraged by all systems. The regionalized framework will distribute computing and provide seamless continuity of operations in the event of a data center failure. MHS will utilize a tiered storage model enabling a reduction in systems load by moving low use records to off line storage. This will also restructure the data to maximize performance for transactions and reporting. The projected number of data centers during this period of performance will be two.

Common Development and Testing Environment (CDE) is currently in the acquisition process which will provide the ability to consolidate multiple, disparate test facilities into one highly configurable environment, thereby:

- Improving software quality and performance
- Reducing incompatibilities between capabilities
- Improving system verification & validation prior to beta testing with the users to minimize defects found in production
- Replicates production environment

Defense Enrollment Eligibility Reporting System is a person-centric system that contains information about all DoD beneficiaries plus information about some people who are not eligible for DoD benefits (e.g. patients and other persons who reside on DEERS for identity purposes). Within DEERS, interfaces with external systems are based on commercial standards where it supports the business requirements or standardized DEERS defined messages where needed. DEERS data provided by DMDC to TMA is also considered protected health information (PHI) as the term is defined in the Home Health System (HHS) Health Insurance Portability and Accountability Act (HIPAA) Privacy Final Rule and accordingly is subject to the requirements of

DoD 6025.18-R which implements that rule for DoD and through the use of TMA business associate agreements to contractors and other non-DoD entities.

Support Activities

These activities are on contract with other vendors and organization and have a relationship in some capacity of potential support. The information is provided for the vendor to clarify their assumptions of what is to be expected and to coordinate activities to prevent disconnects between work done by a vendor or organization to keep the current architecture operational with the activities in this SOO that may have significant architectural changes to stabilize the environment.

The System Integrator supports component integration related tasks. They are responsible for testing the integrated product with the entire EHR suite to ensure interoperability, usability and appropriate data sharing across the continuum of care. The integrator also supports the data center providing management information system support to the common development and test environment for component developers. The integrator supports information assurance in the integrated suite. The Contractor will provide select tier III support for other components that do not work as designed outside of fixing AHLTA/CHCS as described in this SOO. The Contractor will work closely with the integrator to complete the tasks outlined in this SOO and is expected to propose a co-operative strategy to eliminate duplication of efforts, maximize existing resources and at the same time mitigate risks associated with dependencies from supporting integration activities that may be provided by a separate vendor.

The System Sustainer provides local MTF system administrators for CHCS and AHLTA. This includes limited tier II support. The sustainer provides limited tier III support for the current CHCS for defects that do not work as designed. This does not include changes in business practice that require changes in system capabilities which are being addressed in this SOO and partially supported by the CHCS reorganization effort. The sustainer also provides limited deployment support for AHLTA/CHCS system updates which the Contractor may leverage in their proposed strategy to deploy these fixes outlined in this SOO. The proposing vendor will be required to provide sufficient level of deployment support above and beyond the current system sustainment contract that includes the necessary tier III support for successful implementation of this SOO and limited site travel.

DISA currently provides operations support, information assurance management, management of the CDR to include middle-ware support applications and MTF AHLTA LCS. DISA deploys and supports capabilities that will be co-located with the CDR, modifications or updates. This includes but is not limited to the suite of middleware products such as the CDR Sync Server, IE FEPS, CWS FEPS, LCS FEPS, Egate servers, EMSS (Snareworks), BHIE AHLTA among others. They provide updates to the MTF level services that include AHLTA LCS. DISA also provide monitoring and system administration to these systems that do not require tier III support to ensure operational continuity. The Contractor will work with DISA through DHIMS and propose a strategy of what services DISA will be expected to provide as part of their proposal to this SOO.

COTS

These COTS products may be available for re-use or integration in some capacity. Their source code will not be provided as GFI. They may require some integration work in order to support the clinical workflow to achieve the objectives set forth within this SOO.

MHS Inpatient Solution for AHLTA, with emergency department capabilities, eliminates the majority of paper-based inpatient documentation at approximately 21 DoD Military Treatment

Facilities, which accounts for over 57% of the MHS inpatient beds. Additionally, the use of this Inpatient Solution allows for standardization of processes and sharing of documentation across DoD and VA treatment facilities. To increase the availability of clinical information on a shared patient population, DoD and VA collaborated to enable bidirectional access to inpatient documentation from DoD's Interim Inpatient Solution through BHIE. This capability is being expanded under current efforts that will expand the electronic capture of inpatient information to approximately 92% of the Sustaining base inpatient beds.

Single Sign on with Context Management provides a common service that allows users to access multiple systems with a single login and navigate between applications with the same patient (context) to give the feel of an integrated EHR suite compatible with the CA SSO System for FHCC NC. SSO with Context Management will allow users to log into multiple EHR applications without having to enter their credentials multiple times. It will also allow them to view data on the same patient in multiple applications without having to search for that patient when going into a different application. This will provide a tremendous positive usability impact. It will also allow for quicker, more efficient navigation through the EHR systems. The project may support a common identity management service (access, authentication and auditing) that will be a component of the ESB to allow access to the right information at the right time with the appropriate security and auditing.

Enterprise Service Bus will provide an integration framework based on open standards and open architecture that provides fundamental services for capabilities and systems to seamlessly interoperate and share disparate information in a well orchestrated approach using common services and:

- Provides fundamental services for capabilities and systems to seamlessly interoperate and share disparate information in a well orchestrated approach using common services
- Provides a dependable and scalable infrastructure that connects disparate applications and IT resources, mediates their incompatibilities, orchestrates their interactions, and makes them broadly available as capability services for additional uses
- Connects IT resource
- Combines and re-assembles capability services to meet changing requirements without disruption

This will improve performance and reliability of data availability through the Enterprise Service Bus (ESB) to provides a dependable and scalable platform that connects disparate applications, mediates their incompatibilities, orchestrates their interactions, and makes them broadly available as services for re-use

- Leverages information from the initial common services framework and DoD BHIE framework enhancements
- Information framework to support the common user configurable GUI
- Improves open standards-based messaging to provide interoperability with other DOD and VA systems

The MHS ESB aims to make integration and SOA and non-SOA enabled components more productive by providing out-of-the box components for common tasks, be they simple or difficult. This effort will develop, test, integrate and implement fundamental services for complex architectures via an event-driven and standards-based messaging engine across the enterprise. The ESB will provide a dependable and scalable infrastructure that connects disparate applications and IT resources, mediates their incompatibilities, orchestrates their interactions, and makes them broadly available as services for additional uses. The ESB simplifies connection of new

applications, web services, and other technologies, including batch files, application servers, legacy middleware products and packaged applications. This foundation will expose information from all systems for seamless data sharing and interoperability. It will also provide a set of common services re-used by all applications such as authentication, security or terminology mapping.

Automated Duplicate Patient Reduction is an automated tool currently in the acquisition process to reduce patient duplicates from the system. This better supports the continuity of care ensuring the patient's health information can be found with more ease. In industry, it is commonly found that systems contain approximately 12% duplicates prior to implementation of such a solution. With the implementation of this solution, it is expected to reduce the number of duplicates consistent with industry which is approximately 4-5% without human intervention.

Table 1- List of Acronyms

ACRONYMS	DEFINITION
A&I	Artifacts & Images
ACF	Alternate Computing Facility
ACTD	Advanced Concept Technology Demonstration
ADT	Admission-Discharge-Transfer
AFCITA	Air Force Complete Immunization Tracking Application
AHLTA	Not an acronym. AHLTA is a proper noun.
AJAX	Asynchronous JavaScript and XML
AMEDD	Army Medical Department
BH	Behavioral Health
BHIE	Bidirectional Health Information Exchange
CAC	Common Access Card
CCHIT	Commission for Healthcare Information Technology
CCM	Clinical Case Management
CCOW	Clinical Context Object Workgroup
CDA	Clinical Document Architecture
CDA	Corporate Dental Application
CDE	Common Development & Testing Environment
CDM	Clinical Data Mart
CDR	Clinical Data Repository
CDR	Critical Design Review
CDT	Current Dental Terminology
CHCS	Composite Health Care System
CHDR	Clinical Data Repository/Health Data Repository
CM	Context Management
CMMI	Capability Maturity Model Integration
CMS	Content Management System
COTS	Commercial-Off-the-Shelf
CPOE	Computer-based Provider Order Entry
CPT	Current Procedural Terminology
CR	Computed Radiography
CSS2	CDR Synch Server#2
CT	Computerized tomography scan
CWS FEPS	Client Workstation Front End Processors
DBSS	Defense Blood Standard System
DCC-W	Defense Contracting Command-Washington
DDS-W	Dental Data System-Web
DEERS	Defense Enrollment Eligibility Reporting System
DENCAS	Dental Common Access
DES	Disability Evaluation System
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DMHRSi	Defense Medical Human Resources System – Internet
DMLSS	Defense Medical Logistics Standard Support
DNIF	Duty Not Involving/Including Flying
DoD	Department of Defense

ACRONYMS	DEFINITION
DOEHRS	DoD Occupational and Environmental Health Readiness System
DOEHRS-IH	DOEHRS-Industrial Hygiene
DOORS	Dynamic Object Oriented Requirements Systems
DTRS	Deployed Tele-Radiology System
DX	Digital X-Ray
EH	Environmental Health
EHR	electronic health record
EKG	Electrocardiogram
EMSS	Emergency Medical Services System
XML	Extensible Markup Language
ER	Emergency Room
ESB	Enterprise Service Bus
ESF	Electronic Standard Forms
FAR	Federal Acquisition Regulation
FDIS	Final Draft International Standard
FEPS	Front End Processors
FHCC	Federal Health Care Center
FHIE	Federal Health Information Exchange
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GEMS	Global Expeditionary Medical System
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GSA	General Services Administration
GUI	Graphical User Interface
HAIMS	Healthcare Artifact and Image Management System
HART	Health Assessment Review Tool
HART-A	Health Assessment Review Tool Accession
HDR	Health Data Repository
HITSP	Healthcare Informational Technology Standards Panel
HL7	Health Level 7
IA	Information Assurance
ICC	Injury Cause Coding
ICD	International Classification of Diseases
ICDB	Integrated Clinical Data Base
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronic Engineers
IE FEPS	Interface Engine Front End Processors
IM/IT	Information Management/Information Technology
IMR	Individual Medical Readiness
IOS	International Organization for Standardization
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
FHCC NC	James A. Lovell Federal Health Care Center
JMAT	Joint Medical Analysis Tool
JMeWS	Joint Medical Workstation
JSR	Java Specification Request

ACRONYMS	DEFINITION
LCS	Local Cache Server
LCS FEPS	Local Cache Server Front End Processors
LDSI	Laboratory Data Sharing Initiative
LOINC	Logical Observation Identifiers Names and Codes
MC4	Medical Communications for Combat Casualty Care
MDE	Mass Dental Exam
MDM	Master Data Management
MEDPROS	Medical Protection System
MHS	Military Health System
MILVAX	Military Vaccines
MPI	Master Patient Index
mTBI	mild Traumatic Brain Injuries
MRRS	Medical Readiness Reporting System
MSAT	Medical Situational Awareness in the Theater
MTF	Military Treatment Facilities
NCAT	Neurocognitive Assessment Tool
NHIN	Nationwide Health Information Network
OCI	Organizational Conflicts of Interest
O&M	Operations and Maintenance
PACS	Picture Archiving and Communications System
PDA	Personal Digital Assistant
PDHRA	Post-Deployment Health Reassessment
PDR	Preliminary Design Review
PDTS	Pharmacy Data Transaction Service
PHA	Periodic Health Assessment
PHD	Public Health Deployed
PIMR	Personal Information in Medical Research
PKI	Public Key Infrastructure
PMITS	Patient Movement Items Tracking System
PPDHA	Pre- and Post-Deployment Health Assessment Forms Sharing
PRP	Personnel Reliability Program
PRP	Physical Readiness Program
PSR	Periodontal Screening and Recording
SAMS	SNAP Automated Medical System
SARD	System Architecture and Requirements Definition
SCR	Service Change Request
SOA	Service Oriented Architecture
SNOMED	Systematized Nomenclature of Medicine
SOAP	Simple Object Access Protocol
SOI	Service Oriented Infrastructure
SOO	Statement of Objectives
SRD	Systems Requirements Document
SRR	System Requirements Review
SSL	Secure Sockets layer
SSO	Single Sign On
TBI	Traumatic Brain INjury
TC2	TMIP Composite Health Care System (CHCS) Cache

ACRONYMS	DEFINITION
TIMPO	Tri-Service Infrastructure Management Program Office
TMA	TRICARE Management Activity
TMDI	Theater Medical Data Integration
TMDS	Theater Medical Data Store
TMIP	Theater Medical Information Program
TOL	TRICARE Online
TOM	Theater Occupational Module
TPOCS	Third-Party Outpatient Collection System
TRAC2ES	U.S. Transportation Command Regulating and Command & Control Aero-medical Evacuation System
UDDI	Universal Description, Discovery and Integration
UIC	User Identification Code
UIDM	User Identity Management
UMLS	Unified Medical Language System
VA	Department of Veterans Affairs
VA CMOP	VA Consolidated Mail Outpatient Pharmacy
VistA	Veterans Health Information Systems and Technology Architecture
VIP	Very Important People
VLER	Virtual Lifetime Electronic Record
WRSP	Web Services for Remote Portlets
WSDL	Web Service Definition Language
WSN	Web Services Notification
WSRP	Web Services for Remote Portlets

AHLTA & CHCS Critical Fixes Alignment of Objectives to the Architecture White Paper

June 28, 2010

Table of Contents

1.0 EXECUTIVE SUMMARY	1
2.0 AHLTA & CHCS CRITICAL FIXES SOO ARCHITECTURE	3
2.1 COMMON GUI.....	3
2.2 LOCAL SITE CONFIGURATION.....	4
2.2.1 CHCS	4
2.2.2 AHLTA Client.....	4
2.2.3 LCS.....	5
2.3 ENTERPRISE LEVEL INFRASTRUCTURE	6
2.4 COMMON SERVICES.....	7
2.4.1 Identity Management	7
2.5 CDR DATA ACCESS	8
3.0 CURRENT ACTIVITIES UNDER WAY	9

1.0 Executive Summary

The objective of the enterprise is to stabilize and modernize a legacy platform by utilizing industry best practices. This will fit into an evolutionary process whereby the enterprise will transform into a Services Oriented Architecture (SOA) web-centric model. Some of the challenges of our current system are:

- Fragmented architecture
- Disparate data dictionaries
- Many points of failure
- Complex inter-connections
- Disparate systems & interfaces
- Resource intensive design
- Slow system performance
- Antiquated technology (20+ Years old)

The AHLTA & CHCS Critical Fixes and Support Statement of Objectives (SOO) represents the first step in addressing existing technical and functional EHR challenges. It identifies the necessary fixes to the legacy EHR systems and architecture so that the EHR capability will be more reliable, stable, user friendly, and perform with adequate speed. Specifically, this project will accomplish the following:

- Stabilize the DoD EHR and correct problems reported by the healthcare community
- Regionalize the computing infrastructure to increase reliability and availability
- Improve the priority and efficiency of medical communications on DoD networks
- Simplify data sharing with federal partners and across the private sector health care delivery network
- Adopt a new EHR design with open, modular capability, enabled by industry standards
- Build to the MHS Enterprise Architecture which supports fast delivery of capabilities, employs a common dictionary of terms and is flexible enough to take advantage of technology advances
- Stabilize and modernize legacy software and hardware
- Operate in no/low communications environments

The work to be performed in the SOO is organized as a set of overarching and focused objectives:

- Overarching Objectives - System, Program, and Design/Engineering
- Focused Objectives
 - FHCC Enterprise Data Sharing
 - Enterprise Service Bus
 - Enterprise Portal Framework
 - AHLTA/CHCS Stabilization
 - Theater Improvements

Due to the alignment of contracts, some of the capabilities addressed in the SOO are already under contract with other vendors (i.e, a majority of the FHCC Enterprise Data Sharing capabilities), while others are not available that were intended to be delivered and operational (i.e, Enterprise Service Bus and Enterprise Portal Framework).

Therefore, the purpose of this white paper is to provide an architectural view of where the future of the DoD's EHR is headed and discuss the specific areas of the hardware and software architecture the government wants addressed. Additionally, there are contracts underway that will impact the work performed in support of this SOO. This paper outlines these projects and further details on each will be provided as needed by the SOO Contracting Officer Representative (COR).

2.0 AHLTA & CHCS Critical Fixes SOO Architecture

The embedded architecture artifact is a DODAF 2.0 compliant Data Flow Diagram (DFD) which describes the enterprise's direction. The granularity between data flow descriptions varies significantly on the model but should only be used as a visual guide with the Interface Control Document for each system remaining as the authoritative source for the description of each interface.

This architectural artifact provides a high level description of the direction of the enterprise. This is NOT a mandate of how the architecture should look but should be used to understand the current thinking on the future of the enterprise. The government is looking for the vendor to analyze the current issues and suggest solutions for this modernization effort which could differ significantly from this architecture. Several examples of potential solutions are provided within the discussion below. These are suggested as design patterns that fit the problem rather than a solution. The only exception to this is the requirement to use JBOSS as an interim ESB solution until the enterprise ESB is available.



AHLTA SOO View
(SV-04 Data Flow).pd

For each of the sections below a reference is provided which maps to the most relevant objective(s) in the SOO.

2.1 Common GUI

Along the top of the diagram, the common GUI is shown and colored to indicate that it will be provided. This is a product that may need some improvements to be able to handle additional load for enterprise-wide roll out. On this portal, there is a series of portlets represented as system functions. It would be advantageous to have these portlets WSRP compliant to the extent possible. It should be noted that some applications, which are not within the scope of this contract, are envisioned as riding on this common GUI. Although the vendor will not be asked to put these portlets on the portal, the completion of the final system should provide for an intuitive user interface for medical providers. The work being performed as part of the FHCC IOC effort should be leveraged to accomplish the objectives outlined in Objective Set 3 – Leverage Enterprise Portal Framework. This is mapped to the System Objective – “Integrate AHLTA and CHCS into a single cohesive, modular and portable health system using industry best practices and a service oriented approach. Leverage Single Sign On and Context Management (SSO/CM) for functions that are not integrated into this single cohesive system. Ensure that new capabilities are integrated with and added to the recently selected Citrix PasswordManager for SSO and CareFx for CM.”

2.2 Local Site Configuration

The layer below the common GUI shows the software residing at each local site. Each individual site has its own configuration and may have its own home grown applications which are tied to a CHCS host. A recommended approach to the end state is to tie all of these CHCS applications, along with AHLTA modules, to a local ESB that will potentially break these point to point connections and provide a single method to access clinical data at the local level. It is recommended that the local ESB provide full functionality to the local applications/modules while the enterprise ESB should be tailored to sync data between the local sites and the enterprise data stores. The current architecture requires CHCS to be available for AHLTA to operate; the government desires this dependency to be removed. This is mapped to the System Objective – “Stabilize AHLTA/Composite Health Care System (CHCS) for high reliability and availability.”

2.2.1 CHCS

CACHE enables object relational mapping and provides the ability to expose all of the CHCS capabilities/functionality as services. Many of these services have been delivered and the government will provide them to the vendor for evaluation for implementation. The intent is to abstract the CHCS capabilities and encapsulate them in services that are supported by CACHE as objects. These should be JSR 208 compliant web services which tie to the local ESB as well as be directly accessible. This will allow for a more agile approach to future development as the enterprise modernizes its’ architecture. This is mapped to the statement of need in Objective Set 4 – “The functionality in AHLTA and CHCS should be configured to operate as loosely coupled services to reduce dependencies and create a layer of abstraction.”

2.2.2 AHLTA Client

The AHLTA code baseline for the vendor to use is version 3.3 SP1. A list of ancillary System Change Requests (SCRs) and outstanding issues were provided to the vendor as GFI. All of the items need to be evaluated and reviewed with the government to identify which ones will be corrected through architecture changes and the remaining will be prioritized for implementation. For example, automated clinical practice guidelines (ACPGs) are turned off due to the instability of XMLProxy. Once this is corrected, ACPGs may perform as expected, and if not, the code will need to be fixed. The intent is not to add any new features into this baseline, rather ensure what we have is stable and the overall performance is enhanced to the extent possible. This is mapped to the statements of need in Objective Set 4 – “High priority AHLTA defects that have not been addressed (APPENDIX A- EHR System Defects and SCRs) must be repaired.” and “High priority Ancillary services and Essentris EHR Interface and Interoperability SCRs shown in APPENDIX A- EHR System Defects and SCRs must be repaired.”

We need to evaluate the 4.0 baseline only for: modernization/improvements, i.e, health history is migrated to a web module, opportunities to repair defects and simplifying the architecture. This is mapped to the System Objective – “Leverage new functionality from the pre-production AHLTA 4.0 baseline and incorporate into Sustaining Base and Theater baselines (APPENDIX C-AHLTA 4.0 Prototype Baseline Functionality). AHLTA 4.0 pre-production source code, binaries, and documentation will be provided as GFI.”

The client and the LCS contain Visual Basic 6.0 code. The code needs to be evaluated and highly utilized areas need to be converted to .net. This is mapped to the Design/Engineering Objective – “The Contractor is encouraged to present a number of options that may include software repairs, software re-write, code conversion (including automated), web service wrapping, new COTS integration or any combination that will result in a simplified but far more reliable, faster and scalable architecture that help transition the MHS into the future state in a follow on phase.”

We are moving towards virtualization and certain features do not work as expected in a virtual environment which need to be corrected. This is mapped to the System Objective – “Maximize use of virtualization technologies where applicable (licenses will be Government Furnished Equipment (GFE)).”

The Medcin product is currently installed on the AHLTA client. This product needs to be upgraded to the current web-based version and made available to the local ESB which will free up 250Mb on the client. This is mapped to the statement of need in Objective Set 4 - “COTS components such as Medcin, 3M and Oracle must be the current version and the use of modified COTS must be reduced.”

2.2.3 LCS

Some LCS servers are 32-bit machines which do not provide enough bandwidth to handle high volume sites and need to be upgraded to 64-bit. This is mapped to the statement of need in Objective Set 4 - “Client software must be optimized so that it can make best use of a 64 bit environment for virtualization.”

The LCS is currently an inline cache which is a common cause of failure. We need to support a data center model between the LCS and the CDR. In this manner, the AHLTA client will not connect directly with the CDR, but the LCS will store data needed to operate for a period of time without connectivity to the CDR. The requirements for data storage at the local level will be spelled out in more detail by the IM community but will likely include a series summary of documents defined by the HITSP CDA.

Upon syncing periodically (during low usage levels) with the CDR, the LCS will send HL7 messages to a queue where an enterprise service will import the data into the CDR. As part of this data center model, the web services residing on the LCS should be accessible via the local ESB in an easily consumable way for external applications to access. This model will provide transparency to the user in the event connectivity is unavailable to the CDR. This is mapped to the following statement of need in Objective

Set 4 - “System dependencies should be reengineered so that essential capabilities can still be provided when other system components are not available. For example, a provider can still document care if the orders management system is not available. In an extreme example, the system can operate offline if the network connection is severed then resynchronize and continue operations in an online mode.” This is also mapped to the System Objective – “Reduce the complexity of the existing computing framework while increasing the availability, maintainability, and performance. Maintain local off-line functionality (e.g., document care) and eliminate single points of failure e.g. inline caches among a number of other points described.”

2.3 Enterprise Level Infrastructure

The next layer is the enterprise level infrastructure layer. This includes two elements: the enterprise level ESB and the HDD. The HDD is a 3M product that has been the backbone of semantic interoperability for much of the enterprise as well as the foundation of the CDR. It is recommended that this product continue to be used in the near term and it is highly recommended that the product be upgraded to the current market version. This is mapped to the statement of need in Objective Set 4 - “COTS components such as Medcin, 3M and Oracle must be the current version and the use of modified COTS must be reduced.”

The enterprise ESB is part of another contract that will not have congruent timelines with the SOO, but the James A. Lovell Federal Health Care Center (FHCC) JBOSS solution should be leveraged and extended as needed for this contract. This should be implemented utilizing generalized logic and tools that are not JBOSS specific or proprietary. The mediator concept shown here, explicitly calls out two functions that will be performed because they are especially important in fixing the problems within the scope of the SOO. Format transformation is currently performed by the eGate interface engine which is unsupported, has performance and scalability issues, and only transforms HL7 2.2 to 2.3 which limits its reusability. eGate also has a limited developer base which makes new development and maintenance difficult and costly. The data transformation function will be integral in achieving interoperability throughout all of the disparate systems that need to be integrated. Mirth should be evaluated as a replacement to eGate. Although many of the data transformations will need to be mapped, there have already been large amounts of mapping performed by the BHIE/CHDR initiatives that should be leveraged and migrated to the new transformation service. This is mapped to the statement of need in Objective Set 4 - “The current architectural components, such as the interface engines, Front End Processors (FEP), eGate, Clinical Data Repository (CDR) sync server, enhanced Local Cache Server (LCS) capabilities and others should be reengineered using modern industry best practices and replaced with sufficient performance capacity to meet current and projected demands.”

The CITA sync server exchanges flat file info with DEERS, this should be modernized to use web services provided by DEERS. This is mapped to the System Objective - “Leverage Defense Manpower Data Center (DMDC) patient identity management services.”

2.4 Common Services

The common services layer in the architecture diagram shows a variety of different products and applications which should be easily accessible as reusable uniform web services. Existing disparate terminology services, tables and lookup values should be moved into a series of common reusable services that can be easily utilized across all applications and accessible via the enterprise ESB. Some examples of common lookup values are: ICD9 codes, demographic lists, DoD lists (rank, patient category). The values can be cached locally for performance, but the authoritative system of record is the respective terminology service. Differences between current terminology service values across applications will need to be addressed. For example, CHCS may use a different patient category list than AHLTA, however, the list should be consolidated. This is mapped to the statement of need in Objective Set 4 - “Standardized Terminology Service (e.g., Registrations, Demographics and Dispositions) must reduce the need for multiple applications to maintain the same table of data elements (e.g., ICD, CPT, Rank).

Currently, there is limited reach back capability in theater which allows a provider to use Citrix to gain access to an AHLTA client. Although it does not import any data into AHLTA-T, it provides the ability for a remote provider to view the patient’s records in AHLTA. It is the government’s desire to have web services at the enterprise level accessible via the enterprise ESB that enable AHLTA-T clients to pull patient information into the local AHLTA-T databases. This includes, but is not limited to: patient demographics, labs, rads, meds, allergies and previous encounters. This is mapped to the System Objective - “Provide reach-back access to health history when a network connection is available for an integrated enterprise view for both Sustaining Base and Theater (e.g., orders and results).”

The current architecture utilizes the CDR sync servers to push information to the CDR from AHLTA-T. The implementation of this architecture uses legacy code, has poor performance (8 transactions per minute) and is not scalable to accommodate added TC2 inpatient data (planned for deployment). The new version should be lightened, streamlined, have significant performance improvements, and migrated to COTS if possible. The new “sync service” should also be able to pull theater messages from multiple queues (TMIP framework drop folders). This is mapped to the statement of need in Objective Set 4 - “The current architectural components, such as the interface engines, Front End Processors (FEP), eGate, Clinical Data Repository (CDR) sync server, enhanced Local Cache Server (LCS) capabilities and others should be reengineered using modern industry best practices and replaced with sufficient performance capacity to meet current and projected demands.”

2.4.1 Identity Management

Identity management spans both provider and patient. The current provider identification and authorization solution is not an enterprise-based solution. TIMPO’s Joint Active directory is an enterprise- based solution and should be implemented as a replacement to the current security solution (Snareworks). This is mapped to the System Objective –

“Leverage Tri-Service Infrastructure Management Program Office (TIMPO) joint active directory service for user identity management.”

DMDC’s patient identity management services will be used for patient identification across the enterprise to include AHLTA-T. This is mapped to the System Objective – “Leverage Defense Manpower Data Center (DMDC) patient identity management services.”

2.5 CDR Data Access

Currently, a majority of the encounter data is stored in a few tables and primarily all read and write transactions are directed towards the same tablespace. Essentially, there are two repositories, the CDR which is a 3M Care Innovation Suite product and the CDR+ which comprises of custom tables. Both the repositories have different access methods and no hot failover capability. Updating the database to Oracle 11g, implementing Oracle RAC, upgrading the 3M Care Innovation Suite, upgrading Tuxedo services, and partitioning the data will provide higher availability and improve overall performance. The enterprise components primarily run on HP-UX, the desire is to migrate from specialized hardware and software to commodity based hardware and software thus making it easier to distribute resources in the cloud. This is mapped to the statement of need in Objective Set 4 - “COTS components such as Medcin, 3M and Oracle must be the current version and the use of modified COTS must be reduced.”

There are multiple ways of accessing data from the CDR. The 3M product natively uses Tuxedo as transaction services; however, over the years, we’ve migrated away from this and use Tuxedo for connection pools and utilize different ways to get the data in and out of the CDR. One method, XMLProxy, was designed as a prototype, is currently unsupported and has performance and reliability issues. BHIE v5 has object relational mappings using hibernate to access the data. Also, products exist such as Oracle’s SALT 2.0 which will web service enable and encapsulate Tuxedo services so that the business rules which have been written to work with the 3M product can still be used. Ideally, we need to tie all of these methods into a common data access layer with one method of accessing the data such that it is abstracted from Tuxedo, XMLProxy, or any method currently used to access the data. This is mapped to the statement of need in Objective Set 4 - “The functionality in AHLTA and CHCS should be configured to operate as loosely coupled services to reduce dependencies and create a layer of abstraction. These capabilities should be exposed as discrete services that may be used in a portal framework.”

3.0 Current Activities Under Way

The program office manages a portfolio of over 30 systems and applications that are in various stages of the system development life cycle. The vendor needs to be aware of all ongoing efforts that impact the SOO. The most relevant initiatives currently under contract that the vendor needs to align with are described below.

The FHCC Initial Operating Capability (IOC) effort is currently supported by multiple vendors and provides a majority of the functionality outlined in Objective Set 1. The government will provide details to the SOO vendor regarding the statements of need that are not being met as part of the ongoing work.

The Automated Duplicate Patient Merge project addresses the data quality issue of duplicate patient data in the Theater and Garrison data repositories. This is a two-phased effort, the first merging existing duplicate patient data and the second, preventing duplicates from entering the system. Initiate®, a COTS product suite is used to provide this capability. This work needs to be incorporated into the SOO vendor's solution.

The government currently has a contract to stabilize and improve the CDR. Embedded is a summary of the near-term funded and proposed unfunded initiatives. The government is requesting a review of these initiatives and a recommended implementation plan considering all of the items that need to be accomplished in this white paper.



CDR Stabilization
Summary and Follow-